NORMA INTERNACIONAL

ISO 19011

Traducción oficial
Official translation
Traduction officielle

Segunda edición
2011-11-15

# Directrices para la auditoría de los sistemas de gestión

*Guidelines for auditing management systems*

*Lignes directrices pour l'audit des systèmes de management*

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 19011:2011
(traducción oficial)

Versión española publicada en 2012

Publicado en Suiza

# Índice

Página

# Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de las Normas Internacionales normalmente se realiza 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, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar Normas Internacionales. Los Proyectos de Normas Internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como Norma Internacional requiere la aprobación por al menos el 75% de los organismos miembros que emiten voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La Norma ISO 19011 ha sido preparada por el Comité Técnico ISO/TC 176, *Gestión y aseguramiento de la calidad*, Subcomité SC 3, *Tecnologías de apoyo*.

Esta segunda edición anula y sustituye a la primera edición (ISO 19011:2002), que ha sido revisada técnicamente.

Las principales diferencias entre las versiones de 2002 y 2011 de la Norma ISO 19011 son las siguientes:

— el objeto y campo de aplicación se ha ampliado de la auditoría de los sistemas de gestión de la calidad y del medio ambiente a las auditorías de todos los sistemas de gestión;

— se ha aclarado la relación entre las Normas ISO 19011 e ISO/IEC 17021;

— se han introducido los métodos de auditoría a distancia y el concepto de riesgo;

— se ha añadido la confidencialidad como un nuevo principio de auditoría;

— se han reorganizado los capítulos 5, 6 y 7;

— se ha incluido un nuevo Anexo B con información adicional, dando como resultado la eliminación de los recuadros de ayuda;

— se ha fortalecido el proceso de determinación y evaluación de las competencias;

— se han incluido en un nuevo Anexo A ejemplos ilustrativos de los conocimientos y habilidades específicos de la disciplina;

— se encuentran disponibles directrices adicionales en el siguiente sitio Web: www.iso.org/19011auditing

## Prólogo de la versión en español

Esta Norma Internacional ha sido traducida por el Grupo de Trabajo *Spanish Translation Task Group (STTG)* del Comité Técnico ISO/TC 176, *Gestión y aseguramiento de la calidad*, en el que participan representantes de los organismos nacionales de normalización y representantes del sector empresarial de los siguientes países:

Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, España, Estados Unidos de América, México, Perú y Uruguay.

Igualmente, en el citado Grupo de Trabajo participan representantes de COPANT (Comisión Panamericana de Normas Técnicas) y de INLAC (Instituto Latinoamericano de la Calidad).

Esta traducción es parte del resultado del trabajo que el Grupo ISO/TC 176/STTG viene desarrollando desde su creación en el año 1999 para lograr la unificación de la terminología en lengua española en el ámbito de la gestión de la calidad.

## Introducción

Desde la publicación de la primera edición de esta Norma Internacional en 2002, se han publicado varias normas nuevas de sistemas de gestión. Como resultado, ahora existe la necesidad de considerar un alcance más amplio de la auditoría de los sistemas de gestión, así como de proporcionar una orientación más genérica.

En 2006, el comité de ISO para la evaluación de la conformidad (CASCO) desarrolló la Norma ISO/IEC 17021, que establece los requisitos para la certificación de tercera parte de los sistemas de gestión y que se basa parcialmente en las directrices contenidas en la primera edición de esta Norma Internacional.

La segunda edición de la Norma ISO/IEC 17021, publicada en 2011, se amplió para transformar la orientación ofrecida en esta Norma Internacional en requisitos para las auditorías de certificación de sistemas de gestión. Es en este contexto que esta segunda edición de esta Norma Internacional proporciona orientación a todos los usuarios, incluyendo las organizaciones pequeñas y medianas, y se concentra en lo que se denomina comúnmente "auditorías internas" (de primera parte) y "auditorías realizadas por clientes a sus proveedores" (de segunda parte). Aunque aquellos implicados en auditorías de certificación de sistemas de gestión sigan los requisitos de la Norma ISO/IEC 17021:2011, también podrían encontrar útil la orientación de esta Norma Internacional.

La relación entre esta segunda edición de esta Norma Internacional y la Norma ISO/IEC 17021:2011 se muestra en la Tabla 1.

**Tabla 1 – Alcance de esta Norma Internacional y su relación con la Norma ISO/IEC 17021:2011**

| **Auditoría interna** | **Auditoría externa** | |
|---|---|---|
| | **Auditoría al proveedor** | **Auditoría de tercera parte** |
| A veces llamada auditoría de primera parte | A veces llamada auditoría de segunda parte | Para propósitos legales, reglamentarios y similares<br><br>Para certificación (Véanse también los requisitos en la Norma ISO/IEC 17021:2011) |

Esta Norma Internacional no establece requisitos, sino que proporciona orientación sobre la gestión de un programa de auditoría, sobre la planificación y realización de una auditoría del sistema de gestión, así como sobre la competencia y evaluación de un auditor y un equipo auditor.

Las organizaciones pueden operar más de un sistema de gestión formal. Para simplificar la legibilidad de esta Norma Internacional, se prefiere la forma singular de "sistema de gestión", pero el lector puede adaptar la implementación de la orientación a su propia situación particular. Esto también aplica al uso de "persona" y "personas", "auditor" y "auditores".

Se pretende que esta Norma Internacional 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. Sin embargo, los usuarios de esta Norma Internacional pueden aplicar esta orientación al desarrollar sus propios requisitos relacionados con auditorías.

La orientación en esta Norma Internacional también puede usarse con el propósito de la autodeclaración, y puede ser útil para organizaciones que participan en la formación de auditores o en la certificación de personas.

La orientación en esta Norma Internacional 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 y de la naturaleza y complejidad de la organización que se va a auditar, así como de los objetivos y el alcance de las auditorías que se van a realizar.

Esta Norma Internacional introduce el concepto de riesgo en la auditoría de sistemas de gestión. El enfoque adoptado se refiere tanto a los riesgos del proceso de auditoría para alcanzar sus objetivos como al riesgo potencial de la auditoría para interferir con las actividades y procesos del auditado. No proporciona orientación específica para los procesos de gestión del riesgo de la organización, pero reconoce que las organizaciones pueden centrar el esfuerzo de auditoría en cuestiones de importancia para el sistema de gestión.

Esta Norma Internacional adopta el enfoque de que cuando se auditan juntos dos o más sistemas de gestión de distintas disciplinas, esto se denomina “auditoría combinada”. 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.

El capítulo 3 establece los términos y definiciones clave utilizados en esta Norma Internacional. Se ha hecho un gran esfuerzo para asegurarse de que estas definiciones no estén en conflicto con las definiciones utilizadas en otras normas.

El capítulo 4 describe los principios en los que se basa la auditoría. Estos principios ayudan al usuario a comprender la naturaleza esencial de la auditoría y son importantes para comprender la orientación establecida en los capítulos 5 a 7.

El capítulo 5 proporciona orientación sobre el establecimiento y la gestión de un programa de auditoría, el establecimiento de los objetivos del programa de auditoría y la coordinación de las actividades de auditoría.

El capítulo 6 proporciona orientación sobre la planificación y realización de una auditoría de un sistema de gestión.

El capítulo 7 proporciona orientación relativa a la competencia y la evaluación de los auditores y los equipos auditores de sistemas de gestión.

El Anexo A ilustra la aplicación de la orientación del capítulo 7 a distintas disciplinas.

El Anexo B proporciona orientación adicional para auditores sobre la planificación y realización de auditorías.

# Directrices para la auditoría de los sistemas de gestión

## 1 Objeto y campo de aplicación

Esta Norma Internacional proporciona 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 los individuos que participan en el proceso de auditoría, incluyendo a la persona que gestiona el programa de auditoría, los auditores y los equipos auditores.

Es aplicable a todas las organizaciones que necesitan realizar auditorías internas o externas de sistemas de gestión, o gestionar un programa de auditoría.

La aplicación de esta Norma Internacional a otros tipos de auditorías es posible, siempre que se preste especial atención a la competencia específica necesaria.

## 2 Referencias normativas

No se citan referencias normativas. Se incluye este capítulo para conservar una numeración de capítulos idéntica a la utilizada en otras normas de sistemas de gestión ISO.

## 3 Términos y definiciones

Para el propósito de este documento, se aplican los siguientes términos y definiciones.

**3.1**
**auditoría**
proceso sistemático, independiente y documentado para obtener **evidencias de la auditoría** (3.3) y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los **criterios de auditoría** (3.2).

NOTA 1 Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por la propia organización, o en su nombre, para la revisión por la dirección y para otros propósitos internos (por ejemplo, para confirmar la eficacia del sistema de gestión o para obtener información para la mejora del sistema de gestión). Las auditorías internas pueden formar la base para una autodeclaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar libre el auditor de responsabilidades en la actividad que se audita o al estar libre de sesgo y conflicto de intereses.

NOTA 2 Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal 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 autoridades reglamentarias o aquellas que proporcionan la certificación.

NOTA 3 Cuando dos o más sistemas de gestión de disciplinas diferentes (por ejemplo, de la calidad, ambiental, seguridad y salud ocupacional) se auditan juntos, se denomina auditoría combinada.

NOTA 4 Cuando dos o más organizaciones auditoras cooperan para auditar a un único **auditado** (3.7), se denomina auditoría conjunta.

NOTA 5 Adaptado de la Norma ISO 9000:2005, definición 3.9.1.

**3.2**
**criterios de auditoria**
conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la **evidencia de la auditoría** (3.3)

NOTA 1 Adaptado de la Norma ISO 9000:2005, definición 3.9.3.

NOTA 2 Si los criterios de auditoría son requisitos legales (incluyendo los reglamentarios), los términos “ cumple” o no “cumple” se utilizan a menudo en los **hallazgos de auditoría** (3.4).

**3.3**
**evidencia de la auditoría**
registros, declaraciones de hechos o cualquier otra información que es pertinente para los **criterios de auditoría** (3.2) y que es verificable

NOTA La evidencia de la auditoría puede ser cualitativa o cuantitativa.

[ISO 9000:2005, definición 3.9.4]

**3.4**
**hallazgos de la auditoría**
resultados de la evaluación de la **evidencia de la auditoría** (3.3) recopilada frente a los **criterios de auditoría** (3.2)

NOTA 1 Los hallazgos de la auditoría pueden indicar conformidad o no conformidad.

NOTA 2 Los hallazgos de la auditoría pueden conducir a la identificación de oportunidades para la mejora o el registro de buenas prácticas.

NOTA 3 Si los criterios de auditoría se seleccionan de entre los requisitos legales u otros requisitos, el hallazgo de la auditoría se denomina cumplimiento o no cumplimiento.

NOTA 4 Adaptado de la Norma ISO 9000:2005, definición 3.9.5.

**3.5**
**conclusiones de la auditoría**
resultado de una **auditoría** (3.1), tras considerar los objetivos de la auditoría y todos los **hallazgos de la auditoría** (3.4)

NOTA Adaptado de la Norma ISO 9000:2005, definición 3.9.6.

**3.6**
**cliente de la auditoría**
organización o persona que solicita una **auditoría** (3.1)

NOTA 1 En el caso de una auditoría interna, el cliente de la auditoría también puede ser el **auditado** (3.7) o la persona que gestiona el programa de auditoría. Las solicitudes de una auditoría externa pueden provenir de fuentes como autoridades reglamentarias, partes contratantes o clientes potenciales.

NOTA 2 Adaptado de la Norma ISO 9000:2005, definición 3.9.7.

**3.7**
**auditado**
organización que es auditada

[ISO 9000:2005, definición 3.9.8]

**3.8**
**auditor**
persona que lleva a cabo una **auditoría** (3.1)

**3.9**
**equipo auditor**
uno o más **auditores** (3.8) que llevan a cabo una **auditoría** (3.1), con el apoyo, si es necesario, de **expertos técnicos** (3.10).

NOTA 1 A un auditor del equipo se le designa como líder del mismo.

NOTA 2 El equipo auditor puede incluir auditores en formación.

[ISO 9000:2005, definición 3.9.10]

**3.10**
**experto técnico**
persona que aporta conocimientos o experiencia específicos al **equipo auditor** (3.9)

NOTA 1 El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural.

NOTA 2 Un experto técnico no actúa como un **auditor** (3.8) en el equipo auditor.

[ISO 9000:2005, definición 3.9.11]

**3.11**
**observador**
persona que acompaña al **equipo auditor** (3.9) pero que no audita.

NOTA 1 Un observador no es parte del **equipo auditor** (3.9) y no influye ni interfiere en la realización de la **auditoría** (3.1).

NOTA 2 Un observador puede designarse por el **auditado** (3.7), una autoridad reglamentaria u otra parte interesada que testifica la **auditoría** (3.1).

**3.12**
**guía**
persona designada por el **auditado** (3.7) para asistir al **equipo auditor** (3.9)

**3.13**
**programa de auditoría**
detalles acordados para un conjunto de una o más **auditorías** (3.1) planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico

NOTA Adaptado de la Norma ISO 9000:2005, definición 3.9.2.

**3.14**
**alcance de la auditoría**
extensión y límites de una **auditoría** (3.1)

NOTA El alcance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el periodo de tiempo cubierto.

[ISO 9000:2005, definición 3.9.13]

**3.15**
**plan de auditoría**
descripción de las actividades y de los detalles acordados de una **auditoría** (3.1)

[ISO 9000:2005, definición 3.9.12]

**3.16**
**riesgo**
efecto de la incertidumbre sobre los objetivos

NOTA Adaptado de la Guía ISO 73:2009, definición 1.1.

**3.17**
**competencia**
capacidad para aplicar conocimientos y habilidades para alcanzar los resultados pretendidos

NOTA La capacidad implica la aplicación apropiada del comportamiento personal durante el proceso de auditoría.

**3.18**
**conformidad**
cumplimiento de un requisito

[ISO 9000:2005, definición 3.6.1]

**3.19**
**no conformidad**
incumplimiento de un requisito

[ISO 9000:2005, definición 3.6.2]

**3.20**
**sistema de gestión**
sistema para establecer la política y los objetivos y para lograr dichos objetivos

NOTA Un sistema de gestión de una organización puede incluir diferentes sistemas de gestión, tales como un sistema de gestión de la calidad, un sistema de gestión financiera o un sistema de gestión ambiental.

[ISO 9000:2005, definición 3.2.2]

## 4 Principios de auditoría

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 un requisito previo para proporcionar conclusiones de la auditoría que sean pertinentes y suficientes y para permitir a los auditores, trabajando independientemente entre sí, alcanzar conclusiones similares en circunstancias similares.

La orientación dada en los capítulos 5 a 7 se basa en los seis principios señalados a continuación.

a) **Integridad**: el fundamento de la profesionalidad

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

— desempeñar su trabajo con honestidad, diligencia y responsabilidad;

— observar y cumplir todos los requisitos legales aplicables;

— demostrar su competencia al desempeñar su trabajo;

— desempeñar su trabajo de manera imparcial, es decir, permanecer ecuánime y sin sesgo en todas sus acciones;

— ser sensible a cualquier influencia que se pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

b) **Presentación imparcial**: 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.

c) **Debido cuidado profesional**: la aplicación de diligencia y juicio al auditar

Los auditores deberían proceder con el debido cuidado, de acuerdo con 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.

d) **Confidencialidad**: seguridad de la información

Los auditores deberían proceder con discreción en el uso y la protección de la información adquirida en el curso de sus tareas. 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 el interés legítimo del auditado. Este concepto incluye el tratamiento apropiado de la información sensible o confidencial.

e) **Independencia**: 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. Para las auditorías internas, los auditores deberían ser independientes de los responsables operativos de la función que se audita. Los auditores deberían mantener la objetividad a lo largo del proceso de auditoría para asegurarse de que los hallazgos y conclusiones de la auditoría estarán basados sólo en la evidencia de la auditoría.

Para las organizaciones pequeñas, puede que no sea posible que los auditores internos sean completamente independientes de la actividad que se audita, pero deberían hacerse todos los esfuerzos para eliminar el sesgo y fomentar la objetividad.

f) **Enfoque basado en la evidencia**: 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. En general se basará en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un periodo de tiempo delimitado 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.

# 5 Gestión de un programa de auditoría

## 5.1 Generalidades

Una organización que necesita llevar a cabo auditorías debería establecer un programa de auditoría que contribuya a la determinación de la eficacia del sistema de gestión del auditado. El programa de auditoría puede incluir auditorías que tengan en consideración una o más normas de sistemas de gestión, llevadas a cabo de manera individual o combinada.

La alta dirección debería asegurarse de que los objetivos del programa de auditoría se han establecido y que se asigna una o más personas competentes para gestionar el programa de auditoría. El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza de la organización que se audita, así como en la naturaleza, funcionalidad, complejidad y nivel de madurez del sistema de gestión que se va a auditar. Debería darse prioridad a asignar los recursos del programa de auditoría para auditar los asuntos de importancia dentro del sistema de gestión. Estos pueden incluir las características clave de la calidad de un producto o los peligros relativos a la salud y la seguridad, o los aspectos ambientales significativos y su control.

NOTA Este concepto se conoce comúnmente como auditoría en función del riesgo. Esta Norma Internacional no proporciona más orientación sobre la auditoría en función del riesgo.

El programa de auditoría debería incluir la información y los recursos necesarios para organizar y llevar a cabo sus auditorías de forma eficaz y eficiente dentro de los periodos de tiempo especificados y también puede incluir lo siguiente:

— objetivos para el programa de auditoría y para las auditorías individuales;

— alcance/número/tipos/duración/ubicaciones/calendario de las auditorías;

— procedimientos del programa de auditoría;

— criterios de auditoría;

— métodos de auditoría;

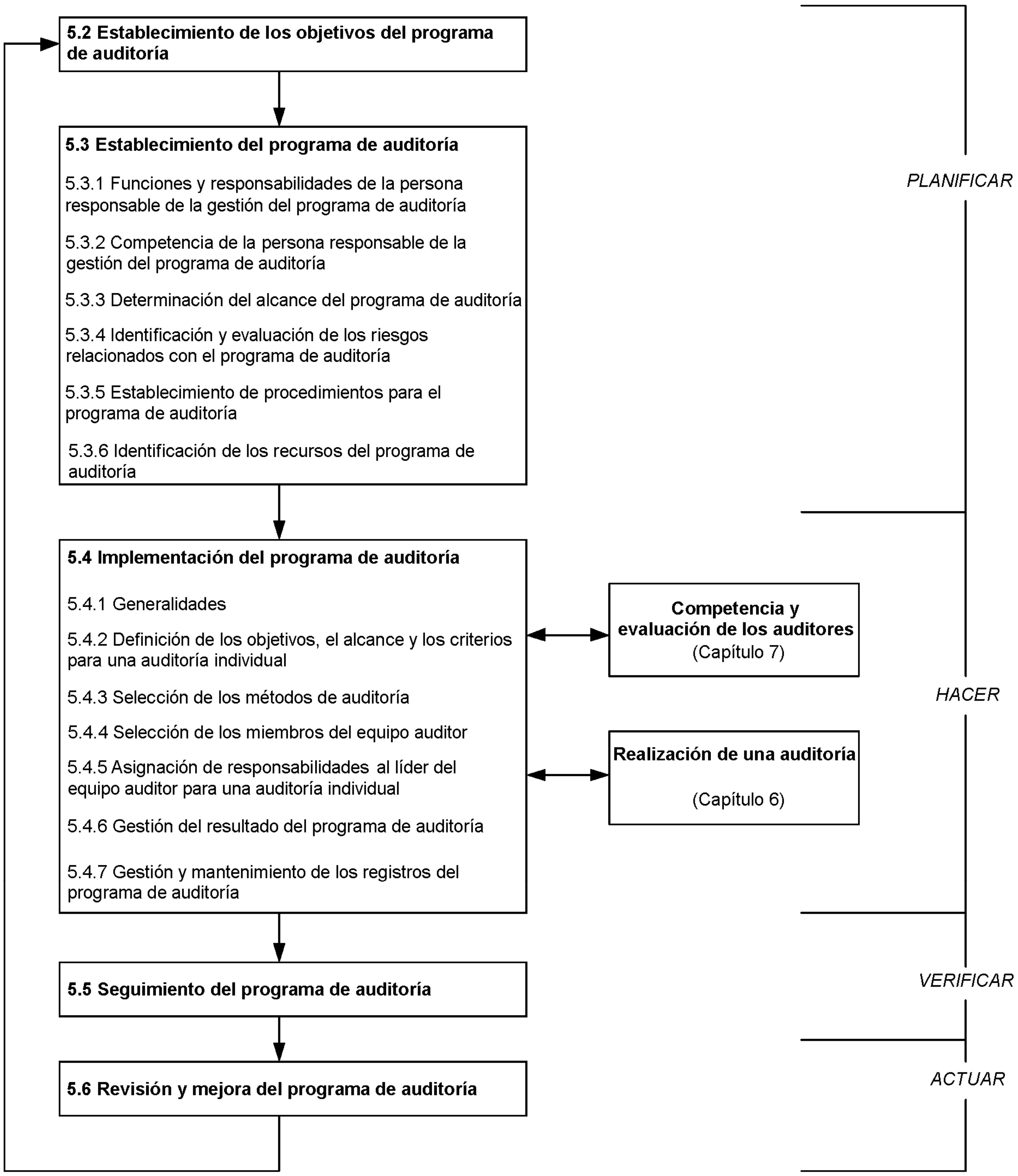
— selección de equipos auditores;

— recursos necesarios, incluyendo viajes y alojamiento;

— procesos para tratar la confidencialidad, la seguridad de la información, la salud y la seguridad y otros asuntos similares.

La implementación del programa de auditoría debería seguirse y medirse para asegurarse de que se han alcanzado sus objetivos. El programa de auditoría debería revisarse para identificar posibles mejoras.

La Figura 1 ilustra el flujo del proceso para la gestión de un programa de auditoría.




NOTA 1 Esta Figura ilustra la aplicación del ciclo Planificar-Hacer-Verificar-Actuar en esta Norma Internacional.

NOTA 2 La numeración de los capítulos/apartados hace referencia a los capítulos/apartados pertinentes de esta Norma Internacional.

**Figura 1 – Diagrama de flujo para la gestión de un programa de auditoría**

## 5.2 Establecimiento de los objetivos del programa de auditoría

La alta dirección debería asegurarse de que los objetivos del programa de auditoría se han establecido para dirigir la planificación y realización de auditorías y debería asegurarse de que el programa de auditoría se ha implementado eficazmente. Los objetivos del programa de auditoría deberían ser coherentes y servir de apoyo a la política y los objetivos del sistema de gestión.

Estos objetivos pueden considerar lo siguiente:

a) prioridades de la dirección;

b) propósitos comerciales y de negocio;

c) características de procesos, productos y proyectos, y cualquier cambio en ellos;

d) requisitos del sistema de gestión;

e) requisitos legales y contractuales y otros requisitos con los que la organización está comprometida;

f) necesidad de evaluar a los proveedores;

g) necesidades y expectativas de partes interesadas, incluyendo los clientes;

h) nivel de desempeño del auditado, como se refleja en la ocurrencia de fallos o incidentes o en quejas de clientes;

i) riesgos para el auditado;

j) resultados de auditorías previas;

k) nivel de madurez del sistema de gestión que se audita.

Ejemplos de objetivos de un programa de auditoría incluyen los siguientes:

— contribuir a la mejora del sistema de gestión y a su desempeño;

— cumplir los requisitos externos, por ejemplo, la certificación con una norma de sistemas de gestión;

— verificar la conformidad con los requisitos contractuales;

— obtener y mantener la confianza en la capacidad de un proveedor;

— determinar la eficacia del sistema de gestión;

— evaluar la compatibilidad y la alineación de los objetivos del sistema de gestión con la política del sistema de gestión y los objetivos globales de la organización.

## 5.3 Establecimiento del programa de auditoría

### 5.3.1 Funciones y responsabilidades de la persona responsable de la gestión del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería:

— establecer el alcance del programa de auditoría;

— identificar y evaluar los riesgos para el programa de auditoría;

— establecer las responsabilidades de la auditoría;

— establecer procedimientos para los programas de auditoría;

— determinar los recursos necesarios;

— asegurarse de la implementación del programa de auditoría, incluyendo el establecimiento de los objetivos, el alcance y los criterios de auditoría de las auditorías individuales, la determinación de los métodos de auditoría y la selección del equipo auditor y la evaluación de los auditores;

— asegurarse de que se gestionan y mantienen los registros apropiados del programa de auditoría;

— seguimiento, revisión y mejora del programa de auditoría.

La persona responsable de la gestión del programa de auditoría debería informar a la alta dirección de los contenidos del programa de auditoría y, cuando sea necesario, solicitar su aprobación.

### 5.3.2 Competencia de la persona responsable de la gestión del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería tener la competencia necesaria para gestionar el programa y sus riesgos asociados de forma eficaz y eficiente, así como conocimientos y habilidades en las siguientes áreas:

— principios, procedimientos y métodos de auditoría;

— normas de sistemas de gestión y documentos de referencia;

— actividades, productos y procesos del auditado;

— requisitos legales y otros requisitos aplicables pertinentes para las actividades y productos del auditado;

— clientes, proveedores y otras partes interesadas del auditado, cuando sea aplicable.

La persona responsable de la gestión del programa de auditoría debería participar en las actividades de desarrollo profesional continuo, apropiadas para mantener los conocimientos y las habilidades necesarios para gestionar el programa de auditoría.

### 5.3.3 Determinación del alcance del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería determinar el alcance del programa de auditoría, que puede variar dependiendo del tamaño y la naturaleza del auditado, así como de la naturaleza, funcionalidad, complejidad y el nivel de madurez del sistema de gestión que se va a auditar, y de asuntos de importancia para el mismo.

NOTA En ciertos casos, dependiendo de la estructura o las actividades de la organización, el programa de auditoría podría consistir únicamente en una auditoría sencilla (por ejemplo, una actividad de un proyecto pequeño).

Otros factores que tienen impacto en un programa de auditoría incluyen los siguientes:

— el objetivo, alcance y duración de cada auditoría y el número de auditorías a llevar a cabo, incluyendo el seguimiento de la auditoría, si es aplicable;

— el número, importancia, complejidad, similitud y la ubicación de las actividades que se van a auditar;

— los factores que influyen en la eficacia del sistema de gestión;

— los criterios de auditoría aplicables, tales como los detalles acordados planificados para los requisitos pertinentes de gestión, de normas, legales y contractuales y otros requisitos con los que la organización está comprometida;

- las conclusiones de auditorías internas o externas previas;
- los resultados de una revisión previa del programa de auditoría;
- el idioma, el contexto cultural y social;
- las preocupaciones de las partes interesadas, tales como quejas de clientes o incumplimiento de los requisitos legales;
- los cambios significativos para el auditado o sus operaciones;
- la disponibilidad de las tecnologías de la información y comunicación para apoyar las actividades de auditoría, en particular el uso de métodos de auditoría a distancia (véase el Anexo B.1);
- la ocurrencia de sucesos internos y externos, tales como fallos del producto, filtraciones en la seguridad de la información, incidentes en materia de salud y seguridad, actos delictivos o incidentes ambientales.

### 5.3.4 Identificación y evaluación de los riesgos relacionados con el programa de auditoría

Hay muchos riesgos distintos asociados con el establecimiento, la implementación, el seguimiento, la revisión y la mejora de un programa de auditoría que pueden afectar al logro de sus objetivos. La persona que gestiona el programa debería considerar estos riesgos en su desarrollo. Estos riesgos pueden asociarse a lo siguiente:

- la planificación, por ejemplo, fallar al establecer objetivos de la auditoría pertinentes y al determinar el alcance del programa de auditoría;
- los recursos, por ejemplo, permitir un tiempo insuficiente para desarrollar el programa de auditoría o llevar a cabo una auditoría;
- la selección del equipo auditor, por ejemplo, el equipo no tiene la competencia colectiva para llevar a cabo auditorías de manera eficaz;
- la implementación, por ejemplo, la comunicación ineficaz del programa de auditoría;
- los registros y sus controles, por ejemplo, fallar al proteger adecuadamente los registros de la auditoría para demostrar la eficacia del programa de auditoría;
- el seguimiento, la revisión y la mejora del programa de auditoría, por ejemplo, el seguimiento ineficaz de los resultados del programa de auditoría.

### 5.3.5 Establecimiento de procedimientos para el programa de auditoría

La persona responsable de la gestión del programa de auditoría debería establecer uno o más procedimientos, tratando lo siguiente, cuando sea aplicable:

- la planificación y elaboración del calendario de las auditorías considerando los riesgos relacionados con el programa de auditoría;
- el aseguramiento de la seguridad y confidencialidad de la información;
- el aseguramiento de la competencia de los auditores y de los líderes de los equipos auditores;
- la selección de los equipos auditores apropiados y la asignación de sus funciones y responsabilidades;
- la realización de las auditorías, incluyendo el uso de métodos de muestreo apropiados;
- la realización del seguimiento de la auditoría, si es aplicable;

— la comunicación a la alta dirección de los logros globales del programa de auditoría;

— la conservación de los registros del programa de auditoría;

— el seguimiento y la revisión del desempeño y de los riesgos, y la mejora de la eficacia del programa de auditoría.

#### 5.3.6 Identificación de los recursos del programa de auditoría

Cuando se identifican los recursos para el programa de auditoría, la persona que gestiona el programa de auditoría debería considerar:

— los recursos financieros necesarios para desarrollar, implementar, gestionar y mejorar las actividades de auditoría;

— los métodos de auditoría;

— la disponibilidad de auditores y expertos técnicos que tengan la competencia apropiada para los objetivos particulares del programa de auditoría;

— el alcance del programa de auditoría y los riesgos relacionados con el programa de auditoría;

— el tiempo y costos de transporte, alojamiento y otras necesidades de la auditoría;

— la disponibilidad de tecnologías de la información y comunicación.

### 5.4 Implementación del programa de auditoría

#### 5.4.1 Generalidades

La persona responsable de la gestión del programa de auditoría debería implementar el programa de auditoría por medio de lo siguiente:

— comunicar las partes pertinentes del programa de auditoría a las partes correspondientes e informarlas periódicamente de su progreso;

— definir los objetivos, el alcance y los criterios para cada auditoría individual;

— coordinar y programar las auditorías y otras actividades relativas al programa de auditoría;

— asegurar la selección de los equipos auditores con la competencia necesaria;

— proporcionar los recursos necesarios para los equipos auditores;

— asegurar la realización de las auditorías de acuerdo con el programa de auditoría y dentro del periodo de tiempo acordado;

— asegurar que se registran las actividades de auditoría y que los registros se gestionan y mantienen adecuadamente;

#### 5.4.2 Definición de los objetivos, el alcance y los criterios para una auditoría individual

Cada auditoría individual debería basarse en unos objetivos, un alcance y unos criterios de auditoría documentados. Estos deberían definirse por la persona que gestiona el programa de auditoría y ser coherentes con los objetivos globales del programa de auditoría.

Los objetivos de la auditoría definen qué es lo que se va a lograr con la auditoría individual y pueden incluir lo siguiente:

— la determinación del grado de conformidad del sistema de gestión que se va a auditar, o de parte de él, con los criterios de auditoría;

— la determinación del grado de conformidad de las actividades, los procesos y los productos con los requisitos y los procedimientos del sistema de gestión;

— la evaluación de la capacidad del sistema de gestión para asegurar el cumplimiento de los requisitos legales y contractuales y de otros requisitos con los que la organización está comprometida;

— la evaluación de la eficacia del sistema de gestión para lograr sus objetivos especificados;

— la identificación de áreas de mejora potencial del sistema de gestión.

El alcance de la auditoría debería ser coherente con el programa de auditoría y con los objetivos de la auditoría. Incluye factores tales como la ubicación, las unidades de la organización, las actividades y los procesos que se van a auditar, así como el periodo de tiempo cubierto por la auditoría.

Los criterios de auditoría se utilizan como una referencia frente a la cual se determina la conformidad, y pueden incluir políticas, objetivos, procedimientos, normas, requisitos legales, requisitos del sistema de gestión, requisitos contractuales, códigos de conducta sectoriales u otros acuerdos planificados aplicables.

Se debería modificar, si es necesario, el programa de auditoría en caso de algún cambio en los objetivos, el alcance o los criterios de la auditoría.

Cuando se auditan juntos dos o más sistemas de gestión de diferentes disciplinas (una auditoría combinada), es importante que los objetivos, el alcance y los criterios de la auditoría sean coherentes con los objetivos de los programas de auditoría pertinentes.

### 5.4.3 Selección de los métodos de auditoría

La persona responsable de la gestión del programa de auditoría debería seleccionar y determinar los métodos para llevar a cabo la auditoría de manera eficaz, dependiendo de los objetivos, el alcance y los criterios de la auditoría definidos.

NOTA En el Anexo B se proporciona orientación sobre cómo determinar los métodos de auditoría.

Cuando dos o más organizaciones auditoras llevan a cabo una auditoría conjunta del mismo auditado, las personas responsables de la gestión de los diferentes programas de auditoría deberían estar de acuerdo en el método de auditoría y considerar las implicaciones para la provisión de recursos y la planificación de la auditoría. Si un auditado opera dos o más sistemas de gestión de disciplinas diferentes, pueden incluirse auditorías combinadas en el programa de auditoría.

### 5.4.4 Selección de los miembros del equipo auditor

La persona responsable de la gestión del programa de auditoría debería designar a los miembros del equipo auditor, incluyendo al líder del equipo y a cualquier experto técnico necesario para la auditoría específica.

Un equipo auditor debería seleccionarse teniendo en cuenta las competencias necesarias para alcanzar los objetivos de la auditoría individual dentro del alcance definido. Si sólo hay un auditor, el auditor debería realizar todas las tareas aplicables a un líder de equipo auditor.

NOTA El capítulo 7 contiene orientación sobre la determinación de las competencias requeridas para los miembros del equipo auditor y describe los procesos para evaluar auditores.

Al decidir el tamaño y la composición del equipo auditor para una auditoría específica, debería considerarse lo siguiente:

a) la competencia global del equipo auditor necesaria para conseguir los objetivos de la auditoría, teniendo en cuenta el alcance y los criterios de la auditoría;

b) la complejidad de la auditoría y si la auditoría es una auditoría combinada o conjunta;

c) los métodos de auditoría que se han seleccionado;

d) los requisitos legales y contractuales y otros requisitos con los que la organización está comprometida;

e) la necesidad de asegurarse de la independencia de los miembros del equipo auditor con respecto a las actividades a auditar y de evitar cualquier conflicto de intereses [véase el principio e) en el capítulo 4];

f) la capacidad de los miembros del equipo auditor para interactuar eficazmente con los representantes del auditado y para trabajar juntos;

g) el idioma de la auditoría, y las características sociales y culturales del auditado. Estos aspectos pueden tratarse bien a través de las habilidades propias del auditor o a través del apoyo de un experto técnico.

Para asegurar la competencia global del equipo auditor, deberían llevarse a cabo los siguientes pasos:

— la identificación de los conocimientos y habilidades necesarios para alcanzar los objetivos de la auditoría;

— la selección de los miembros del equipo auditor, de tal manera que el conjunto de conocimientos y habilidades necesarios esté presente en el equipo auditor.

Si los auditores del equipo auditor no cubren todas las competencias necesarias, deberían incluirse en el equipo expertos técnicos con competencias adicionales. Los expertos técnicos deberían operar bajo la dirección de un auditor, pero no deberían actuar como auditores.

Los auditores en formación pueden incluirse en el equipo auditor, pero deberían participar bajo la dirección y orientación de un auditor.

Durante la auditoría pueden ser necesarios ajustes en el tamaño y la composición del equipo auditor, es decir, si surge un conflicto de intereses o un problema de competencia. Si surge una situación tal, debería discutirse con las partes apropiadas (por ejemplo, el líder del equipo auditor, la persona responsable de la gestión del programa de auditoría, el cliente de la auditoría o el auditado) antes de que se realice ningún ajuste.

#### 5.4.5 Asignación de responsabilidades al líder del equipo auditor para una auditoría individual

La persona responsable de la gestión del programa de auditoría debería asignar a un líder del equipo auditor la responsabilidad de llevar a cabo la auditoría individual.

La asignación debería hacerse con tiempo suficiente antes de la fecha programada de la auditoría, para asegurarse de la planificación eficaz de la auditoría.

Para asegurarse de la realización eficaz de las auditorías individuales, debería proporcionarse al líder del equipo auditor la siguiente información:

a) los objetivos de la auditoría;

b) los criterios de auditoría y cualquier documento de referencia;

c) el alcance de la auditoría, incluyendo la identificación de las unidades de la organización y unidades funcionales y los procesos que se van a auditar;

d) los métodos y procedimientos de la auditoría;

e) la composición del equipo auditor;

f) los detalles de contacto con el auditado, las ubicaciones, fechas y duración de las actividades de auditoría que se van a llevar a cabo;

g) la asignación de los recursos apropiados para llevar a cabo la auditoría;

h) la información necesaria para evaluar y tratar los riesgos identificados para el logro de los objetivos de la auditoría.

Esta información también debería cubrir lo siguiente, cuando sea apropiado:

— el idioma de trabajo y del informe de la auditoría, cuando sea diferente del idioma del auditor o del auditado;

— el contenido y la distribución del informe de auditoría requerido por el programa de auditoría;

— los asuntos relacionados con la confidencialidad y la seguridad de la información, si lo requiere el programa de auditoría;

— los requisitos de salud y seguridad para los auditores;

— los requisitos de seguridad y de autorización;

— las acciones de seguimiento, por ejemplo, respecto de una auditoría previa, si es aplicable;

— la coordinación con otras actividades de auditoría, en caso de una auditoría conjunta.

Cuando se lleva a cabo una auditoría conjunta es importante alcanzar un acuerdo entre las organizaciones que llevan a cabo las auditorías, antes de que la auditoría comience, sobre las responsabilidades específicas de cada parte, especialmente en lo que concierne a la autoridad del líder del equipo auditor designado para la auditoría.

### 5.4.6 Gestión del resultado del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería asegurarse de que se realizan las siguientes actividades:

— la revisión y aprobación de los informes de la auditoría, incluyendo la evaluación de la idoneidad y adecuación de los hallazgos de la auditoría;

— la revisión del análisis de la causa raíz y de la eficacia de las acciones correctivas y las acciones preventivas;

— la distribución de informes de auditoría a la alta dirección y a otras partes pertinentes;

— la determinación de la necesidad de alguna auditoría de seguimiento.

### 5.4.7 Gestión y mantenimiento de los registros del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería asegurarse de que se crean, gestionan y mantienen registros de la auditoría para demostrar la implementación del programa de auditoría. Deberían establecerse procesos para asegurarse de que se trata cualquier necesidad de confidencialidad asociada con los registros de la auditoría.

Los registros deberían incluir lo siguiente:

a) los registros relacionados con el programa de auditoría, tales como:

— los objetivos y el alcance del programa de auditoría documentados;

— los relativos a los riesgos relacionados con el programa de auditoría;

— las revisiones de la eficacia del programa de auditoría;

b) los registros relacionados con cada auditoría individual, tales como:

— los planes de auditoría y los informes de auditoría;

— los informes de no conformidad;

— los informes de acciones correctivas y preventivas;

— los informes de seguimiento de la auditoría, si es aplicable;

c) los registros relacionados con el personal de auditoría que cubre temas tales como:

— la evaluación de la competencia y el desempeño de los miembros del equipo auditor;

— la selección de los equipos auditores y los miembros del equipo;

— el mantenimiento y la mejora de la competencia.

La forma y el nivel de detalle de los registros deberían demostrar que se han alcanzado los objetivos del programa de auditoría.

## 5.5 Seguimiento del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería seguir su implementación considerando la necesidad de:

a) evaluar la conformidad con los programas de auditoría, calendarios y objetivos de la auditoría;

b) evaluar el desempeño de los miembros del equipo auditor;

c) evaluar la capacidad de los equipos auditores para implementar el plan de auditoría;

d) evaluar la retroalimentación de la alta dirección, de los auditados, de los auditores y de otras partes interesadas;

Algunos factores pueden determinar la necesidad de modificar el programa de auditoría, tales como los siguientes:

— los hallazgos de la auditoría;

— el nivel demostrado de eficacia del sistema de gestión;

— los cambios en el sistema de gestión del cliente o del auditado;

— los cambios en las normas, los requisitos legales y contractuales y otros requisitos con los que la organización está comprometida;

— el cambio de proveedor.

### 5.6 Revisión y mejora del programa de auditoría

La persona responsable de la gestión del programa de auditoría debería revisar el programa de auditoría para evaluar si se han alcanzado sus objetivos. Las lecciones aprendidas de la revisión del programa de auditoría deberían usarse como elementos de entrada para el proceso de mejora continua para el programa.

La revisión del programa de auditoría debería considerar lo siguiente:

a) los resultados y tendencias del seguimiento del programa de auditoría;

b) la conformidad con los procedimientos del programa de auditoría;

c) la evolución de las necesidades y expectativas de las partes interesadas;

d) los registros del programa de auditoría;

e) los métodos de auditoría alternativos o nuevos;

f) la eficacia de las medidas para tratar los riesgos asociados con el programa de auditoría;

g) los temas de confidencialidad y seguridad de la información relacionados con el programa de auditoría;

La persona responsable de la gestión del programa de auditoría debería revisar la implementación global del programa de auditoría, identificar las áreas de mejora, modificar el programa si es necesario, y también debería:

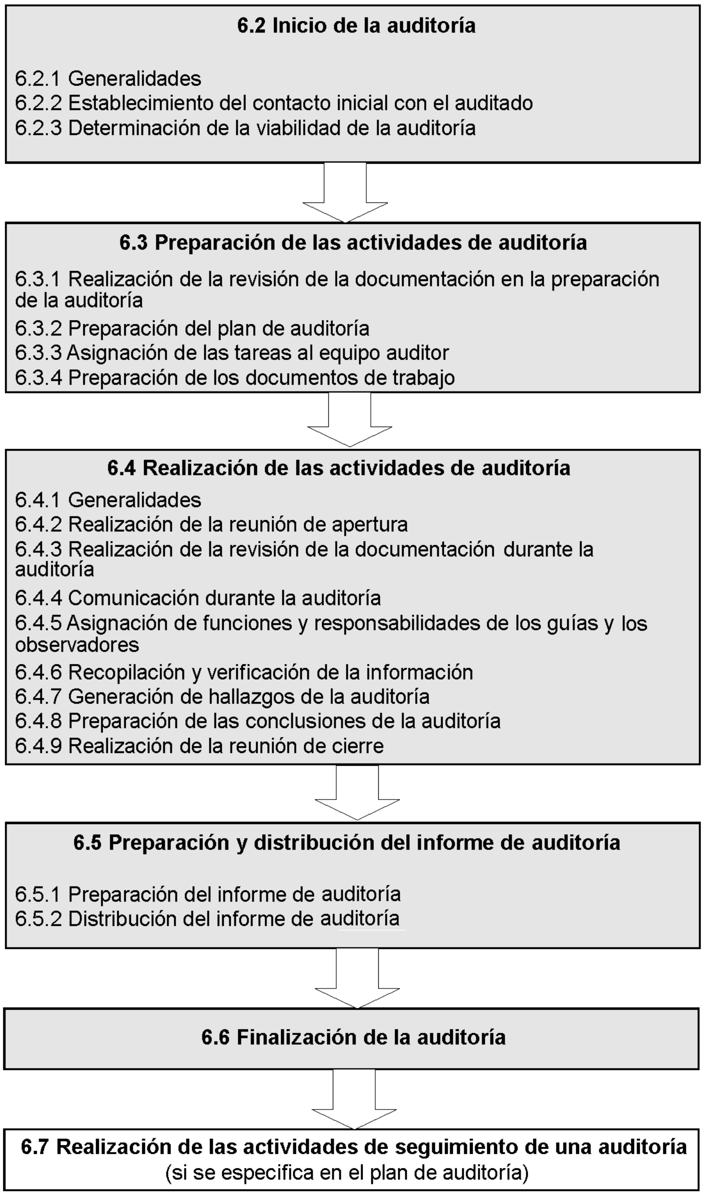
— revisar el desarrollo profesional continuo de los auditores, de acuerdo con 7.4, 7.5 y 7.6;

— informar a la alta dirección de los resultados de la revisión del programa de auditoría.

## 6 Realización de una auditoría

### 6.1 Generalidades

Este capítulo contiene orientación sobre la preparación y realización de actividades de auditoría como parte de un programa de auditoría. La Figura 2 proporciona una visión general de las actividades de auditoría típicas. El grado de aplicación de las disposiciones de este capítulo depende de los objetivos y del alcance de la auditoría específica.




NOTA La numeración hace referencia a los apartados pertinentes de esta Norma Internacional.

**Figura 2 – Actividades típicas de auditoría**

## 6.2 Inicio de la auditoría

### 6.2.1 Generalidades

Cuando se inicia una auditoría, la responsabilidad de llevar a cabo la auditoría corresponde al líder del equipo auditor designado (véase 5.4.5) hasta que la auditoría finaliza (véase 6.6).

Para iniciar una auditoría, deberían considerarse los pasos de la Figura 2; sin embargo, la secuencia puede diferir dependiendo del auditado, de los procesos y de las circunstancias específicas de la auditoría.

### 6.2.2 Establecimiento del contacto inicial con el auditado

El contacto inicial con el auditado para la realización de la auditoría puede ser informal o formal y debería realizarse por el líder del equipo auditor. Los propósitos del contacto inicial son los siguientes:

— establecer comunicaciones con los representantes del auditado;

— confirmar la autoridad para llevar a cabo la auditoría;

— proporcionar información sobre los objetivos de la auditoría, el alcance, los métodos y la composición del equipo auditor, incluyendo los expertos técnicos;

— solicitar acceso a los documentos y registros pertinentes con propósitos de planificación;

— determinar los requisitos legales y contractuales aplicables y otros requisitos pertinentes para las actividades y productos del auditado;

— confirmar lo acordado con el auditado respecto al grado de difusión y al tratamiento de la información confidencial;

— hacer los preparativos para la auditoría incluyendo la programación de las fechas;

— determinar los requisito específicos de la ubicación en cuanto al acceso seguridad, salud y protección u otros requisitos especiales;

— acordar la asistencia de observadores y la necesidad de guías para el equipo auditor;

— determinar cualquier área de interés o preocupación para el auditado en relación con la auditoría específica.

### 6.2.3 Determinación de la viabilidad de la auditoría

Debería determinarse la viabilidad de la auditoría para proporcionar la confianza razonable en que los objetivos de la auditoría pueden alcanzarse.

La determinación de la viabilidad debería tener en cuenta factores tales como la disponibilidad de lo siguiente:

— la información suficiente y apropiada para planificar y llevar a cabo la auditoría;

— la cooperación adecuada del auditado;

— el tiempo y los recursos adecuados para llevar a cabo la auditoría.

Cuando la auditoría no es viable, debería proponerse al cliente de la auditoría una alternativa, de acuerdo con el auditado.

## 6.3 Preparación de las actividades de auditoría

### 6.3.1 Realización de la revisión de la documentación en la preparación de la auditoría

Debería revisarse la documentación pertinente del sistema de gestión del auditado para:

— reunir información para preparar las actividades de auditoría y los documentos de trabajo aplicables (véase 6.3.4), por ejemplo, sobre procesos, funciones;

— establecer una visión general del grado de la documentación del sistema para detectar posibles carencias;

NOTA  Se proporciona orientación sobre cómo realizar una revisión de la documentación en el capítulo B.2.

La documentación debería incluir, cuando sea aplicable, documentos y registros del sistema de gestión, así como informes de auditorías previas. La revisión de la documentación debería tener en cuenta el tamaño, la naturaleza y la complejidad del sistema de gestión y de la organización del auditado, así como los objetivos y el alcance de la auditoría.

### 6.3.2 Preparación del plan de auditoría

**6.3.2.1** El líder del equipo auditor debería preparar un plan de auditoría basado en la información contenida en el programa de auditoría y en la documentación proporcionada por el auditado. El plan de auditoría debería considerar el efecto de las actividades de auditoría en los procesos del auditado y proporcionar la base para el acuerdo entre el cliente de la auditoría, el equipo auditor y el auditado en lo relativo a la realización de la auditoría. El plan debería facilitar la programación en el tiempo y la coordinación eficientes de las actividades de auditoría a fin de alcanzar los objetivos.

El nivel de detalle proporcionado en el plan de auditoría debería reflejar el alcance y la complejidad de ésta, así como el efecto de la incertidumbre en el logro de los objetivos de la auditoría. Al preparar el plan de auditoría, el líder del equipo auditor debería ser consciente de lo siguiente:

— las técnicas de muestreo apropiadas (véase el capítulo B.3);

— la composición del equipo auditor y su competencia colectiva;

— los riesgos para la organización creados por la auditoría.

Por ejemplo, pueden originarse riesgos para la organización por la presencia de los miembros del equipo auditor que influyen en la salud y la seguridad, el entorno y la calidad, y su presencia puede presentar amenazas para los productos, servicios, personal o infraestructura del auditado (por ejemplo, contaminación de espacios limpios).

Para las auditorías combinadas, debería prestarse especial atención a las interacciones entre los procesos operativos y los objetivos y prioridades que concurren en los distintos sistemas de gestión.

**6.3.2.2** El grado de detalle y el contenido del plan de auditoría pueden diferir, por ejemplo, entre la auditoría inicial y las posteriores, así como entre las auditorías internas y externas. El plan de auditoría debería ser lo suficientemente flexible para permitir los cambios que pueden hacerse necesarios a medida que las actividades de auditoría se vayan llevando a cabo.

El plan de auditoría debería cubrir o hacer referencia a lo siguiente:

a) los objetivos de la auditoría;

b) el alcance de la auditoría, incluyendo la identificación de las unidades de la organización y unidades funcionales, así como los procesos que van a auditarse;

c) los criterios de auditoría y cualquier documento de referencia;

d) las ubicaciones, las fechas, el horario y la duración previstos de las actividades de auditoría que se van a llevar a cabo, incluyendo las reuniones con la dirección del auditado;

e) los métodos de auditoría que se van a usar, incluyendo el grado en que se necesita el muestreo de la auditoría para obtener las evidencias de auditoría suficientes y el diseño del programa de muestreo, si es aplicable;

f) las funciones y responsabilidades de los miembros del equipo auditor, así como los guías y los observadores;

g) la asignación de los recursos apropiados para las áreas críticas de la auditoría.

El plan de auditoría también puede cubrir lo siguiente, cuando sea apropiado:

— la identificación del representante del auditado en la auditoría;

— el idioma de trabajo y del informe de la auditoría, cuando sea diferente del idioma del auditor o del auditado;

— los temas del informe de la auditoría;

— los preparativos logísticos y de comunicaciones, incluyendo los preparativos específicos para las ubicaciones que se van a auditar;

— las medidas específicas a tomar para tratar el efecto de la incertidumbre en el logro de los objetivos de la auditoría;

— los asuntos relacionados con la confidencialidad y la seguridad de la información;

— las acciones de seguimiento a partir de una auditoría previa;

— las actividades de seguimiento de la auditoría planificada;

— la coordinación con otras actividades de auditoría, en el caso de una auditoría conjunta.

El plan de auditoría puede ser revisado y aceptado por el cliente de la auditoría, y debería presentarse al auditado. Cualquier objeción por parte del auditado sobre el plan de auditoría debería resolverse entre el líder del equipo auditor, el auditado y el cliente de la auditoría.

#### 6.3.3 Asignación de las tareas al equipo auditor

El líder del equipo auditor, consultando con el equipo auditor, debería asignar a cada miembro del equipo la responsabilidad para auditar procesos, actividades, funciones o lugares específicos. Tales asignaciones deberían tener en cuenta la independencia y la competencia de los auditores y el uso eficaz de los recursos, así como las diferentes funciones y responsabilidades de los auditores, los auditores en formación y los expertos técnicos.

El líder del equipo auditor debería realizar reuniones informativas del equipo auditor, cuando sea apropiado, para distribuir las asignaciones de trabajo y decidir los posibles cambios. Los cambios en las asignaciones de trabajo pueden hacerse a medida que la auditoría se va llevando a cabo para asegurarse del logro de los objetivos de la auditoría.

#### 6.3.4 Preparación de los documentos de trabajo

Los miembros del equipo auditor deberían recopilar y revisar la información pertinente a las tareas de auditoría asignadas y preparar los documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría. Tales documentos de trabajo pueden incluir lo siguiente:

— listas de verificación;

— planes de muestreo de auditoría;

— formularios para registrar la información, tales como evidencias de apoyo, hallazgos de la auditoría y registros de las reuniones.

El uso de listas de verificación y formularios no debería restringir la extensión de las actividades de auditoría, que pueden cambiarse como resultado de la información recopilada durante la auditoría.

NOTA Se proporciona orientación sobre la preparación de documentos de trabajo en el capítulo B.4.

Los documentos de trabajo, incluyendo los registros que resultan de su uso, deberían retenerse al menos hasta que finalice la auditoría, o según se especifique en el plan de auditoría. La retención de los documentos después de finalizada la auditoría se describe en el apartado 6.6. Aquellos documentos que contengan información confidencial o protegida deberían salvaguardarse de manera adecuada en todo momento por los miembros del equipo auditor.

## 6.4 Realización de las actividades de auditoría

### 6.4.1 Generalidades

Normalmente las actividades de auditoría se realizan en una secuencia definida como se indica en la Figura 2. Esta secuencia puede variar para adaptarse a las circunstancias de auditorías específicas.

### 6.4.2 Realización de la reunión de apertura

El propósito de la reunión de apertura es:

a) confirmar el acuerdo de todas las partes (por ejemplo, auditado, equipo auditor) sobre el plan de auditoría,

b) presentar al equipo auditor, y

c) asegurarse de que se pueden realizar todas las actividades de auditoría planificadas.

Debería celebrarse una reunión de apertura con la dirección del auditado y, cuando sea apropiado, con aquellos responsables de las funciones o de los procesos que se van a auditar. Durante la reunión, debería proporcionarse la oportunidad de realizar preguntas.

El grado de detalle debería ser coherente con la familiaridad del auditado con el proceso de auditoría. En muchos casos, por ejemplo, en auditorías internas en una organización pequeña, la reunión de apertura puede consistir simplemente en comunicar que se está realizando una auditoría y explicar la naturaleza de la auditoría.

Para otras situaciones de auditoría, la reunión puede ser formal y se debería mantener registro de los asistentes. El líder del equipo auditor debería presidir la reunión, y deberían considerarse los siguientes puntos, cuando sea apropiado:

— presentación de los participantes, incluyendo los observadores y los guías, y una descripción general de sus funciones;

— confirmación de los objetivos, alcance y criterios de la auditoría;

— confirmación del plan de auditoría y de otras disposiciones pertinentes con el auditado, como la fecha y hora de la reunión de cierre, cualquier reunión intermedia entre el equipo auditor y la dirección del auditado, y cualquier cambio de última hora;

— presentación de los métodos que se van a utilizar para realizar la auditoría, incluyendo la aclaración al auditado de que la evidencia de la auditoría se basará en una muestra de la información disponible;

— presentación de los métodos para gestionar los riesgos para la organización que pueden resultar de la presencia de los miembros del equipo auditor;

— confirmación de los canales de comunicación formal entre el equipo auditor y el auditado;

— confirmación del idioma que se va a utilizar durante la auditoría;

— confirmación de que, durante la auditoría, el auditado será informado del progreso de la misma;

— confirmación de que los recursos e instalaciones que necesita el equipo auditor están disponibles;

— confirmación de los temas relacionados con la confidencialidad y la seguridad de la información;

— confirmación de los procedimientos pertinentes para el equipo auditor relativos a salud y protección, emergencia y seguridad;

— información del método de presentación de la información sobre hallazgos de la auditoría incluyendo la categorización, si la hay;

— información acerca de las condiciones bajo las cuales la auditoría puede darse por terminada;

— información acerca de la reunión de cierre;

— información acerca de cómo tratar los posibles hallazgos durante la auditoría;

— información acerca de cualquier sistema de retroalimentación del auditado sobre los hallazgos o conclusiones de la auditoría, incluyendo las quejas o apelaciones.

#### 6.4.3 Realización de la revisión de la documentación durante la auditoría

La documentación pertinente del auditado debería revisarse para:

— determinar la conformidad del sistema con los criterios de auditoría, con base en la documentación disponible;

— reunir información para apoyar las actividades de auditoría.

NOTA Se proporciona orientación sobre cómo realizar una revisión de la documentación en el capítulo B.2.

La revisión puede combinarse con otras actividades de auditoría y puede continuar a lo largo de la auditoría, siempre que no perjudique a la eficacia de la auditoría.

Si no puede proporcionarse la documentación adecuada dentro del periodo de tiempo dado en el plan de auditoría, el líder del equipo auditor debería informar tanto al responsable de la gestión del programa de auditoría como al auditado. Dependiendo de los objetivos y el alcance de la auditoría, debería tomarse una decisión sobre si la auditoría debería continuar o suspenderse hasta que se resuelvan los problemas relativos a la documentación.

#### 6.4.4 Comunicación durante la auditoría

Durante la auditoría, puede ser necesario llegar a acuerdos formales para la comunicación dentro del equipo auditor, así como con el auditado, el cliente de la auditoría y potencialmente con organismos externos (por ejemplo, autoridades reglamentarias), especialmente cuando los requisitos legales exijan la comunicación obligatoria de los no cumplimientos.

El equipo auditor debería reunirse periódicamente para intercambiar información, evaluar el progreso de la auditoría y reasignar las tareas entre los miembros del equipo auditor, según sea necesario.

Durante la auditoría, el líder del equipo auditor debería comunicar periódicamente los progresos de la auditoría y cualquier inquietud al auditado y, cuando sea apropiado, al cliente de la auditoría. Las evidencias recopiladas durante la auditoría que sugieren un riesgo inmediato y significativo para el auditado deberían comunicarse sin demora al auditado y, si es apropiado, al cliente de la auditoría. Cualquier inquietud relacionada con un aspecto externo al alcance de la auditoría debería registrarse y notificarse al líder del equipo auditor, para su posible comunicación al cliente de la auditoría y al auditado.

Cuando las evidencias de la auditoría disponibles indican que los objetivos de la misma no son alcanzables, el líder del equipo auditor debería informar de las razones al cliente de la auditoría y al auditado para determinar las acciones apropiadas. Estas acciones pueden incluir la reconfirmación o la modificación del plan de auditoría, cambios en los objetivos de la auditoría o en su alcance, o la finalización de la auditoría.

Cualquier necesidad de cambios en el plan de auditoría que pueda evidenciarse a medida que las actividades de auditoría progresan debería revisarse y aprobarse, cuando sea apropiado, tanto por la persona responsable de la gestión del programa de auditoría como por el auditado.

#### 6.4.5 Asignación de funciones y responsabilidades de los guías y los observadores

Los guías y los observadores (por ejemplo, una autoridad reglamentaria u otras partes interesadas) pueden acompañar al equipo auditor. No deberían influir ni interferir en la realización de la auditoría. Si esto no se puede asegurar, el líder del equipo auditor debería tener el derecho de negarse a que los observadores tomen parte en ciertas actividades de auditoría.

Para los observadores, cualquier obligación en relación con la salud y la protección, la seguridad y la confidencialidad debería gestionarse entre el cliente de la auditoría y el auditado.

Los guías, designados por el auditado, deberían asistir al equipo auditor y actuar cuando lo solicite el líder del equipo auditor. Sus responsabilidades deberían incluir lo siguiente:

a) ayudar a los auditores a identificar a las personas que participarán en las entrevistas y a confirmar los horarios;

b) acordar el acceso a ubicaciones específicas del auditado;

c) asegurarse de que las reglas concernientes a los procedimientos relacionados con la protección y la seguridad de las ubicaciones, son conocidas y respetadas por los miembros del equipo auditor y los observadores.

La función del guía también puede incluir lo siguiente:

— ser testigos de la auditoría en nombre del auditado;

— proporcionar aclaraciones o ayudar en la recopilación de la información.

#### 6.4.6 Recopilación y verificación de la información

Durante la auditoría, debería recopilarse mediante un muestreo apropiado y verificarse la información pertinente a los objetivos, el alcance y los criterios de la misma, incluyendo la información relativa a las interrelaciones entre funciones, actividades y procesos. Sólo la información que es verificable debería aceptarse como evidencia de la auditoría. Debería registrarse la evidencia que conduce a hallazgos de la auditoría. Si, durante la recopilación de evidencias, el equipo auditor es consciente de cualquier circunstancia de riesgo nueva o que ha cambiado, el equipo debería tratarlo en consecuencia.

NOTA 1 Se proporciona orientación sobre muestreo en el capítulo B.3.

La Figura 3 proporciona una visión general del proceso, desde la recopilación de información hasta las conclusiones de la auditoría.

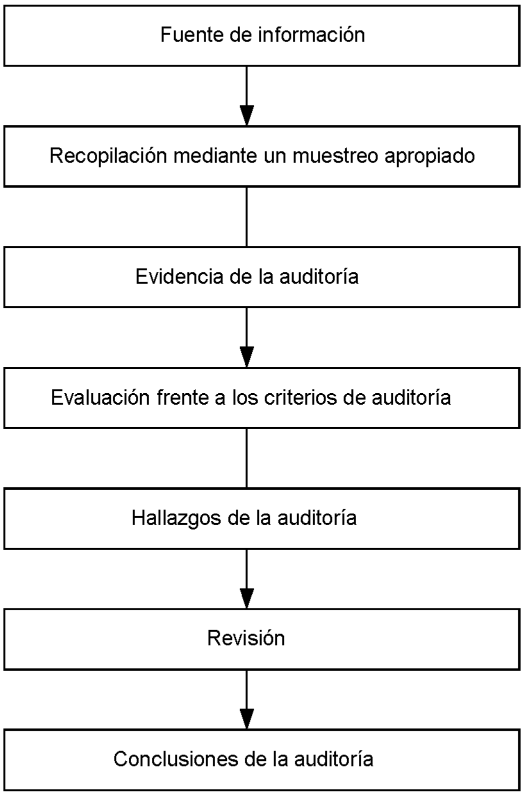



**Figura 3 – Visión general del proceso de recopilación y verificación de la información**

Los métodos para recopilar la información incluyen lo siguiente:

— entrevistas;

— observaciones;

— revisión de documentos, incluyendo los registros.

NOTA 2 Se proporciona orientación sobre las fuentes de información en el capítulo B.5.

NOTA 3 Se proporciona orientación sobre las visitas a la ubicación del auditado en el capítulo B.6.

NOTA 4 Se proporciona orientación sobre cómo realizar entrevistas en el capítulo B.7.

#### 6.4.7 Generación de hallazgos de la auditoría

La evidencia de la auditoría debería evaluarse frente a los criterios de auditoría para determinar los hallazgos de la auditoría. Los hallazgos de la auditoría pueden indicar conformidad o no conformidad con los criterios de auditoría. Cuando lo especifique el plan de auditoría, los hallazgos de una auditoría individual deberían incluir la conformidad y las buenas prácticas junto con la evidencia que los apoya, las oportunidades de mejora y cualquier recomendación para el auditado.

Deberían registrarse las no conformidades y la evidencia de la auditoría que las apoya. Las no conformidades pueden clasificarse. Deberían revisarse con el auditado para reconocer que la evidencia de la auditoría es exacta y que las no conformidades se han comprendido. Se debería realizar todo el esfuerzo posible para resolver cualquier opinión divergente relativa a las evidencias o a los hallazgos de la auditoría, y deberían registrarse los puntos para los que no haya acuerdo.

El equipo auditor debería reunirse, según sea necesario, para revisar los hallazgos de la auditoria en etapas apropiadas durante la auditoría.

NOTA Se proporciona orientación adicional sobre la identificación y evaluación de los hallazgos de la auditoría en el capítulo B.8.

### 6.4.8 Preparación de las conclusiones de la auditoría

El equipo auditor debería reunirse antes de la reunión de cierre para:

a) revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma;

b) acordar las conclusiones de la auditoría, teniendo en cuenta la incertidumbre inherente al proceso de auditoría;

c) preparar recomendaciones, si estuviera especificado en el plan de auditoría;

d) comentar el seguimiento de la auditoría, cuando sea aplicable.

Las conclusiones de la auditoría pueden tratar aspectos tales como los siguientes:

— el grado de conformidad y el reconocimiento de la fortaleza del sistema de gestión con los criterios de auditoría, incluyendo la eficacia del sistema de gestión para cumplir los objetivos establecidos;

— la implementación, el mantenimiento y la mejora eficaces del sistema de gestión;

— la capacidad del proceso de revisión por la dirección para asegurar la continua idoneidad, adecuación, eficacia y mejora del sistema de gestión;

— el logro de los objetivos de la auditoría, cobertura del alcance de la auditoría y cumplimiento de los criterios de la auditoría;

— las causas raíz de los hallazgos, si se incluyen en el plan de auditoría;

— hallazgos similares encontrados en distintas áreas que se auditaron con el propósito de identificar tendencias.

Si se especifica en el plan de auditoría, las conclusiones de auditoría pueden llevar a recomendaciones para la mejora, o a futuras actividades de auditoría.

### 6.4.9 Realización de la reunión de cierre

La reunión de cierre, facilitada por el líder del equipo auditor, debería realizarse para presentar los hallazgos y las conclusiones de la auditoría. Entre los participantes en la reunión de cierre debería incluirse a los representantes de la dirección del auditado y, cuando sea apropiado, a aquellos responsables de las funciones o procesos que se han auditado, y también puede incluirse al cliente de la auditoría y otras partes. Si es aplicable, el líder del equipo auditor debería prevenir al auditado de las situaciones encontradas durante la auditoría que pueden disminuir la confianza en las conclusiones de la auditoría. Si está definido en el sistema de gestión o por acuerdo con el cliente de la auditoría, los participantes deberían acordar el periodo de tiempo para un plan de acción que trate los hallazgos de la auditoría.

El grado de detalle debería ser coherente con la familiaridad del auditado con el proceso de auditoría. Para algunas situaciones de auditoría, la reunión puede ser formal y las actas, incluyendo los registros de asistencia, deberían conservarse. En otras situaciones, por ejemplo, en auditorías internas, la reunión de cierre es menos formal y puede consistir sólo en comunicar los hallazgos de la auditoría y las conclusiones de la misma.

Cuando sea apropiado, en la reunión de cierre debería explicarse al auditado lo siguiente:

— aclarar que la evidencia de la auditoría recopilada se basó en una muestra de la información disponible;

— el método de presentación de la información;

— el proceso de tratamiento de los hallazgos de la auditoría y sus posibles consecuencias;

— la presentación de los hallazgos y conclusiones de la auditoría de tal manera que se comprendan y se reconozcan por la dirección del auditado;

— todas las actividades posteriores a la auditoría relacionadas (por ejemplo, implementación de acciones correctivas, tratamiento de quejas de la auditoría, proceso de apelación).

Cualquier opinión divergente relativa a los hallazgos de la auditoría o las conclusiones entre el equipo auditor y el auditado debería discutirse y, si es posible, resolverse. Si no se resuelve, deberían registrarse todas las opiniones.

Si lo especifican los objetivos de la auditoría, pueden presentarse recomendaciones para la mejora. Se debería enfatizar que las recomendaciones no tienen carácter vinculante.

## 6.5 Preparación y distribución del informe de auditoría

### 6.5.1 Preparación del informe de auditoría

El líder del equipo auditor debería informar de los resultados de la auditoría de acuerdo con los procedimientos del programa de auditoría.

El informe de auditoría debería proporcionar un registro completo, preciso, conciso y claro de la auditoría, y debería incluir o hacer referencia a lo siguiente:

a) los objetivos de la auditoría;

b) el alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados;

c) la identificación del cliente de la auditoría;

d) la identificación del equipo auditor y de los participantes del auditado en la auditoría;

e) las fechas y ubicaciones donde se realizaron las actividades de auditoría;

f) los criterios de auditoría;

g) los hallazgos de la auditoría y las evidencias relacionadas;

h) las conclusiones de la auditoría;

i) una declaración del grado en el que se han cumplido los criterios de la auditoría;

El informe de la auditoría también puede incluir o hacer referencia a lo siguiente, cuando sea apropiado:

— el plan de auditoría, incluyendo el horario;

— un resumen del proceso de auditoría, incluyendo cualquier obstáculo encontrado que pueda disminuir la confianza en las conclusiones de la auditoría;

— la confirmación de que se han cumplido los objetivos de la auditoría dentro del alcance de la auditoría, de acuerdo con el plan de auditoría;

— cualquier área dentro del alcance de la auditoría no cubierta;

— un resumen cubriendo las conclusiones de la auditoría y los principales hallazgos de la auditoría que las apoyan;

— las opiniones divergentes sin resolver entre el equipo auditor y el auditado;

— las oportunidades para la mejora, si se especifica en el plan de auditoría;

— las buenas prácticas identificadas;

— los planes de acción del seguimiento acordados, si los hubiera;

— una declaración sobre la naturaleza confidencial de los contenidos;

— cualquier implicación para el programa de auditoría o las auditorías posteriores;

— la lista de distribución del informe de la auditoría.

NOTA El informe de auditoría puede elaborarse antes de la reunión de cierre.

### 6.5.2 Distribución del informe de auditoría

El informe de auditoría debería emitirse en el periodo de tiempo acordado. Si se retrasa, las razones deberían comunicarse al auditado y a la persona responsable de la gestión del programa de auditoría.

El informe de auditoría debería estar fechado, revisado y aprobado, cuando sea apropiado, de acuerdo con los procedimientos del programa de auditoría.

A continuación, el informe de la auditoría debería distribuirse a los receptores, tal y como se define en los procedimientos de auditoría o en el plan de auditoría.

## 6.6 Finalización de la auditoría

La auditoría finaliza cuando se hayan realizado todas las actividades de auditoría planificadas, o si se ha acordado de otro modo con el cliente de la auditoría (por ejemplo, podría haber una situación inesperada que impida que la auditoría se finalice de acuerdo con el plan).

Los documentos pertenecientes a la auditoría deberían conservarse o destruirse de común acuerdo entre las partes participantes y de acuerdo con los procedimientos del programa de auditoría y los requisitos aplicables.

Salvo que se requiera por ley, el equipo auditor y la persona que gestiona el programa de auditoría no deberían revelar el contenido de los documentos, otra información obtenida durante la auditoría ni el informe de auditoría a ninguna otra parte, sin la aprobación explícita del cliente de la auditoría y, cuando sea apropiado, la del auditado. Si se requiere revelar el contenido de un documento de la auditoría, el cliente de la auditoría y el auditado deberían ser informados tan pronto como sea posible.

Las lecciones aprendidas de la auditoría deberían incorporarse al proceso de mejora continua del sistema de gestión de las organizaciones auditadas.

### 6.7 Realización de las actividades de seguimiento de una auditoría

Las conclusiones de la auditoría pueden, dependiendo de los objetivos de la auditoría, indicar la necesidad de correcciones, o de acciones correctivas, preventivas o de mejora. Tales acciones generalmente son decididas y emprendidas por el auditado en un intervalo de tiempo acordado. Cuando sea apropiado, el auditado debería mantener informada a la persona responsable de la gestión del programa de auditoría y al equipo auditor sobre el estado de estas acciones.

Debería verificarse si se completaron las acciones y su eficacia. Esta verificación puede ser parte de una auditoría posterior.

## 7 Competencia y evaluación de los auditores

### 7.1 Generalidades

La confianza en el proceso de auditoría y la capacidad de lograr sus objetivos depende de la competencia de aquellos individuos que participen en la planificación y realización de las auditorías, incluyendo los auditores y líderes de equipos auditores. La competencia debería evaluarse a través de un proceso que considere el comportamiento personal y la capacidad para aplicar los conocimientos y las habilidades adquiridos durante la educación, la experiencia laboral, la formación como auditor y la experiencia en auditorías. Este proceso debería tener en cuenta las necesidades del programa de auditoría y sus objetivos. Algunos de los conocimientos y habilidades descritos en 7.2.3 son comunes a los auditores de cualquier disciplina de sistema de gestión; otros son específicos de disciplinas de sistemas de gestión individuales. No es necesario que cada auditor en el equipo auditor tenga la misma competencia; sin embargo, la competencia global del equipo auditor necesita ser suficiente para lograr los objetivos de la auditoría.

La evaluación de la competencia del auditor debería planificarse, implementarse y documentarse de acuerdo con el programa de auditoría, incluyendo los procedimientos para proporcionar un resultado que es objetivo, coherente, imparcial y fiable. El proceso de evaluación debería incluir cuatro pasos principales, como se indica a continuación:

a) determinar la competencia del personal de auditoría para cumplir las necesidades del programa de auditoría;

b) establecer los criterios de evaluación;

c) seleccionar el método de evaluación apropiado;

d) realizar la evaluación.

El resultado del proceso de evaluación debería proporcionar la base para lo siguiente:

— la selección de los miembros del equipo auditor como se describe en 5.4.4;

— la determinación de la necesidad de mejorar la competencia (por ejemplo, formación adicional);

— la evaluación continua del desempeño de los auditores.

Los auditores deberían desarrollar, mantener y mejorar su competencia mediante el desarrollo profesional continuo y la participación regular en auditorías (véase 7.6).

Se describe un proceso para evaluar a los auditores y a los líderes de equipos auditores en 7.4 y 7.5.

Los auditores y los líderes de equipos auditores deberían ser evaluados respecto a los criterios establecidos en 7.2.2 y 7.2.3.

La competencia requerida de la persona responsable de la gestión del programa de auditoría se describe en 5.3.2.

## 7.2 Determinación de la competencia del auditor para cumplir las necesidades del programa de auditoría

### 7.2.1 Generalidades

Al decidir los conocimientos y habilidades apropiados requeridos al auditor, debería considerarse lo siguiente:

— el tamaño, naturaleza y complejidad de la organización que se va a auditar;

— las disciplinas del sistema de gestión que se va a auditar;

— los objetivos y amplitud del programa de auditoría;

— otros requisitos, tales como los impuestos por organismos externos, cuando sea apropiado;

— la función del proceso de auditoría en el sistema de gestión del auditado;

— la complejidad del sistema de gestión que se va a auditar;

— la incertidumbre en el logro de los objetivos de la auditoría.

Esta información debería compararse con lo enumerado en 7.2.3.2, 7.2.3.3 y 7.2.3.4.

### 7.2.2 Comportamiento personal

Los auditores deberían poseer las cualidades necesarias que les permitan actuar de acuerdo con los principios de la auditoría tal como se describe en el capítulo 4. Los auditores deberían demostrar un comportamiento profesional durante el desempeño de las actividades de auditoría, incluyendo ser:

— ético, es decir, imparcial, sincero, honesto y discreto;

— de mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos;

— diplomático, es decir, con tacto en las relaciones con las personas;

— observador, es decir, activamente consciente del entorno físico y las actividades;

— perceptivo, es decir, consciente y capaz de entender las situaciones;

— versátil, es decir, capaz de adaptarse fácilmente a diferentes situaciones;

— tenaz, es decir, persistente y orientado hacia el logro de los objetivos;

— decidido, es decir, capaz de alcanzar conclusiones oportunas basadas en el análisis y el razonamiento lógico;

— seguro de sí mismo, es decir, capaz de actuar y funcionar independientemente a la vez que interactúa eficazmente con otros;

— firme, es decir, capaz de actuar de manera responsable y ética, aunque estas acciones puedan no ser siempre populares y en alguna ocasión puedan causar desacuerdos o alguna confrontación;

— abierto a la mejora, es decir, dispuesto a aprender de las situaciones, y que se esfuerza por conseguir mejores resultados de auditoría;

— abierto a las diferencias culturales, es decir, observador y respetuoso con la cultura del auditado;

— colaborador, es decir, que interactúa eficazmente con los demás, incluyendo los miembros del equipo auditor y el personal del auditado.

### 7.2.3 Conocimientos y habilidades

#### 7.2.3.1 Generalidades

Los auditores deberían poseer los conocimientos y las habilidades necesarios para obtener los resultados previstos de las auditorías que se espera que lleven a cabo. Todos los auditores deberían poseer conocimientos y habilidades genéricos y también se debería esperar que tuvieran conocimientos y habilidades específicos de alguna disciplina y algún sector. Los líderes del equipo auditor deberían tener los conocimientos y habilidades adicionales necesarios para dirigir al equipo auditor.

#### 7.2.3.2 Conocimientos y habilidades genéricos de los auditores de sistemas de gestión

Los auditores deberían tener conocimientos y habilidades de las áreas señaladas a continuación.

a) **Principios, procedimientos y métodos de auditoría**: los conocimientos y habilidades en esta área permiten al auditor aplicar los principios, procedimientos y métodos apropiados a las diferentes auditorías, y asegurarse de que las auditorías se realizan de manera coherente y sistemática. Un auditor debería ser capaz de hacer lo siguiente:

   — aplicar principios, procedimientos y métodos de auditoría;

   — planificar y organizar el trabajo eficazmente;

   — llevar a cabo la auditoría dentro del horario acordado;

   — establecer prioridades y centrarse en los temas de importancia;

   — recopilar información, mediante entrevistas eficaces, escuchando, observando y revisando documentos, registros y datos;

   — comprender y tener en consideración las opiniones de los expertos;

   — comprender lo apropiado de utilizar técnicas de muestreo para las auditorías, y sus consecuencias;

   — verificar la pertinencia y exactitud de la información recopilada;

   — confirmar que la evidencia de la auditoría es suficiente y apropiada para apoyar los hallazgos y conclusiones de la auditoría;

   — evaluar los factores que pueden afectar a la fiabilidad de los hallazgos y conclusiones de la auditoría;

   — utilizar documentos de trabajo para registrar las actividades de auditoría;

   — documentar los hallazgos de la auditoría y preparar los informes de auditoría apropiados;

   — mantener la confidencialidad y seguridad de la información, los datos, los documentos y los registros;

   — comunicarse eficazmente, oralmente y por escrito (personalmente, o mediante el uso de intérpretes y traductores);

   — comprender los tipos de riesgos asociados con la auditoría.

b) **Sistema de gestión y documentos de referencia**: los conocimientos y habilidades en esta área permiten al auditor comprender el alcance de la auditoría y aplicar los criterios de auditoría, y deberían cubrir lo siguiente:

— las normas de sistemas de gestión u otros documentos usados como criterios de auditoría;

— la aplicación de normas de sistemas de gestión por parte del auditado y de otras organizaciones, cuando sea apropiado;

— la interacción entre los componentes del sistema de gestión;

— el reconocimiento de la jerarquía de los documentos de referencia;

— la aplicación de los documentos de referencia a las diferentes situaciones de auditoría.

c) **Contexto de la organización**: los conocimientos y habilidades en esta área permiten al auditor comprender la estructura, las actividades y las prácticas de gestión del auditado, y deberían cubrir lo siguiente:

— los tipos, gobernabilidad, tamaño, estructura, funciones y relaciones de la organización;

— los conceptos generales del negocio y de la gestión, los procesos y la terminología relacionada, incluyendo la planificación, la preparación de presupuestos y la gestión del personal;

— el contexto cultural y social del auditado.

d) **Requisitos legales y contractuales aplicables y otros requisitos que aplican al auditado**: los conocimientos y las habilidades en esta área permiten al auditor ser consciente de los requisitos legales y contractuales de la organización y trabajar con ellos. Los conocimientos y las habilidades específicos de la jurisdicción o de las actividades y productos del auditado deberían cubrir lo siguiente:

— las leyes y los reglamentos y las autoridades reglamentarias asociadas;

— la terminología legal básica;

— los contratos y la responsabilidad legal.

#### 7.2.3.3 Conocimientos y habilidades específicos de la disciplina y del sector de los auditores de sistemas de gestión

Los auditores deberían tener los conocimientos y las habilidades específicos de la disciplina y del sector que son apropiados para auditar el tipo particular de sistema de gestión y el sector.

No es necesario que cada auditor en el equipo auditor tenga la misma competencia; sin embargo, la competencia global del equipo de auditoría necesita ser la suficiente para alcanzar los objetivos de la auditoría.

Los conocimientos y las habilidades específicos de la disciplina y del sector de los auditores incluyen lo siguiente:

— los requisitos y principios del sistema de gestión específicos de la disciplina, y su aplicación;

— los requisitos legales pertinentes para la disciplina y el sector, tales como que el auditor sea consciente de los requisitos específicos para la jurisdicción y de las obligaciones, las actividades y los productos del auditado;

— los requisitos de las partes interesadas pertinentes para la disciplina específica;

— los fundamentos de la disciplina y la aplicación de métodos, técnicas, procesos y prácticas de negocio y técnicas específicas de la disciplina, suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

— los conocimientos específicos de la disciplina relativos al sector particular, la naturaleza de las operaciones o el lugar de trabajo que se audita, suficientes para que el auditor evalúe las actividades, procesos y productos (bienes y servicios) del auditado;

— los principios, los métodos y las técnicas de gestión de riesgos pertinentes para la disciplina y el sector, tales que el auditor pueda evaluar y controlar los riesgos asociados con el programa de auditoría.

NOTA Se proporciona orientación y ejemplos ilustrativos de los conocimientos y habilidades específicos de la disciplina para los auditores en el Anexo A.

#### 7.2.3.4 Conocimientos y habilidades genéricos del líder de un equipo auditor

Los líderes de los equipos auditores deberían tener conocimientos y habilidades adicionales para gestionar y proporcionar liderazgo al equipo auditor, para facilitar la realización eficiente y eficaz de la auditoría. Un líder de equipo auditor debería tener los conocimientos y habilidades necesarios para hacer lo siguiente:

a) equilibrar las fortalezas y debilidades de los miembros individuales del equipo auditor;

b) desarrollar una relación de trabajo armoniosa entre los miembros del equipo auditor;

c) gestionar el proceso de auditoría, incluyendo:

  — planificar la auditoría y hacer un uso eficaz de los recursos durante la auditoría;

  — gestionar la incertidumbre de lograr los objetivos de la auditoría;

  — proteger la salud y la seguridad de los miembros del equipo auditor durante la auditoría, incluyendo asegurar el cumplimiento de los auditores con los requisitos pertinentes de salud, protección y seguridad;

  — organizar y dirigir a los miembros del equipo auditor;

  — proporcionar dirección y orientación a los auditores en formación;

  — prevenir y resolver conflictos, cuando sea necesario;

d) representar al equipo auditor en las comunicaciones con la persona responsable de la gestión del programa de auditoría, el cliente de la auditoría y el auditado;

e) liderar el equipo auditor para alcanzar las conclusiones de la auditoría;

f) preparar y completar el informe de la auditoría.

#### 7.2.3.5 Conocimientos y habilidades para auditar sistemas de gestión que tratan múltiples disciplinas

Los auditores que pretenden participar como miembro de un equipo auditor en la auditoría de sistemas de gestión que tratan múltiples disciplinas deberían tener la competencia necesaria para auditar al menos una de las disciplinas de sistema de gestión y conocimientos de la interacción y sinergia entre los distintos sistemas de gestión.

Los líderes de equipos auditores que realizan auditorías de sistemas de gestión que tratan múltiples disciplinas deberían comprender los requisitos de cada una de las normas de sistemas de gestión y reconocer los límites de sus conocimientos y habilidades en cada una de las disciplinas.

### 7.2.4 Logro de la competencia del auditor

Los conocimientos y habilidades del auditor pueden obtenerse usando una combinación de lo siguiente:

— educación formal/formación y experiencia que contribuya al desarrollo de los conocimientos y habilidades en la disciplina y en el sector del sistema de gestión que el auditor pretende auditar;

— programas de formación que cubren los conocimientos y habilidades genéricos del auditor;

— experiencia en una función técnica, de gestión o profesional que implique el ejercicio del juicio, la toma de decisiones, la solución de problemas y la comunicación con miembros de la dirección, profesionales, pares, clientes y otras partes interesadas;

— experiencia en auditorías adquirida bajo la supervisión de un auditor en la misma disciplina.

### 7.2.5 Líderes de los equipos auditores

Un líder de equipo auditor debería haber adquirido experiencia adicional en auditoría para desarrollar los conocimientos y habilidades descritos en 7.2.3. Esta experiencia adicional debería haberse adquirido trabajando bajo la dirección y orientación de un líder de equipo auditor diferente.

## 7.3 Establecimiento de los criterios de evaluación del auditor

Los criterios deberían ser cualitativos (tales como haber demostrado el comportamiento personal, los conocimientos o el desempeño de las habilidades, en la formación o en el lugar de trabajo) y cuantitativos (tales como los años de experiencia laboral y de educación, el número de auditorías realizadas, las horas de formación en auditoría).

## 7.4 Selección del método apropiado de evaluación del auditor

La evaluación debería llevarse a cabo usando dos o más de los métodos seleccionados entre los indicados en la Tabla 2. Al utilizar la Tabla 2, se debería tener en cuenta lo siguiente:

— los métodos señalados representan una variedad de opciones que pueden no ser aplicables en todas las situaciones;

— los diversos métodos señalados pueden diferir en su fiabilidad;

— debería utilizarse una combinación de métodos para asegurar un resultado objetivo, coherente, imparcial y fiable.

**Tabla 2 – Métodos de evaluación posibles**

| Método de evaluación | Objetivos | Ejemplos |
|---|---|---|
| Revisión de registros | Verificar los antecedentes del auditor | Análisis de los registros de educación, formación, laborales, credenciales profesionales y experiencia en auditorías |
| Retroalimentación | Proporcionar información sobre cómo se percibe el desempeño del auditor | Encuestas, cuestionarios, referencias personales, recomendaciones, quejas, evaluación del desempeño, evaluación entre pares |
| Entrevista | Evaluar el comportamiento personal y las habilidades de comunicación, para verificar la información y examinar los conocimientos, y para obtener información adicional | Entrevistas personales |
| Observación | Evaluar el comportamiento personal y la aptitud para aplicar los conocimientos y habilidades | Juego de roles, auditorías en presencia de un testigo, desempeño en una situación real |
| Examen | Evaluar el comportamiento personal y los conocimientos y habilidades y su aplicación | Exámenes orales y escritos, exámenes psicotécnicos |
| Revisión después de la auditoría | Proporcionar información sobre el desempeño del auditor durante las actividades de auditoría, identificar fortalezas y debilidades | Revisión del informe de la auditoría, entrevistas con el líder del equipo auditor, el equipo auditor y, si es apropiado, retroalimentación del auditado. |

## 7.5 Realización de la evaluación del auditor

La información recopilada sobre la persona debería compararse con los criterios establecidos en 7.2.3. Cuando una persona que se espera que participe en un programa de auditoría no cumple los criterios, entonces debería adquirir una formación, experiencia laboral o experiencia en auditoría adicional, y debería realizarse posteriormente una nueva evaluación.

## 7.6 Mantenimiento y mejora de la competencia del auditor

Los auditores y los líderes de equipos auditores deberían mejorar su competencia de manera continua. Los auditores deberían mantener su competencia en auditoría a través de la participación regular en auditorías de sistemas de gestión y del desarrollo profesional continuo. El desarrollo profesional continuo implica el mantenimiento y la mejora de la competencia. Esto puede conseguirse a través de medios como experiencia laboral adicional, formación, estudios particulares, tutorías, asistencia a reuniones, seminarios y conferencias u otras actividades pertinentes.

La persona responsable de la gestión del programa de auditoría debería establecer los mecanismos adecuados para la evaluación continua del desempeño de los auditores, y de los líderes de equipos auditores.

Las actividades de desarrollo profesional continuo deberían tener en cuenta lo siguiente:

— los cambios en las necesidades del individuo y de la organización responsable de la realización de la auditoría;

— las técnicas de auditoría;

— las normas pertinentes y otros requisitos.

# Anexo A
(informativo)

# Orientación y ejemplos ilustrativos de conocimientos y habilidades de un auditor en disciplinas específicas

## A.1 Generalidades

Este Anexo proporciona ejemplos genéricos de conocimientos y habilidades específicos de una disciplina para auditores de sistemas de gestión, que se pretende sirvan como orientación para ayudar a la persona responsable de la gestión del programa de auditoría a seleccionar o evaluar a los auditores.

Otros ejemplos de conocimientos y habilidades específicos de una disciplina para auditores también pueden desarrollarse para los sistemas de gestión. Se sugiere que, cuando sea posible, dichos ejemplos sigan la misma estructura general para asegurar la posibilidad de comparación.

## A.2 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de la seguridad en los transportes

Los conocimientos y habilidades relacionados con la gestión de la seguridad en los transportes y la aplicación de métodos, técnicas, procesos y prácticas de gestión de la seguridad en los transportes deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— la terminología relativa a la gestión de la seguridad;

— la comprensión del enfoque basado en el sistema de seguridad;

— la evaluación y la mitigación del riesgo;

— el análisis de los factores humanos relacionados con la gestión de la seguridad en los transportes;

— el comportamiento humano y la interacción;

— la interacción de personas, máquinas, procesos y el ambiente de trabajo;

— los peligros potenciales y otros factores del lugar de trabajo que afectan a la seguridad;

— los métodos y prácticas para la investigación de incidentes y el seguimiento del desempeño de la seguridad;

— la evaluación de incidentes y accidentes de las operaciones;

— el desarrollo de medidas del desempeño proactivas y reactivas y de métricas.

NOTA Para más información, véase la futura Norma ISO 39001 desarrollada por el Comité Técnico ISO/PC 241 sobre sistemas de gestión de la seguridad del tráfico por carretera.

## A.3 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión ambiental

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

- la terminología ambiental;
- las métricas y estadísticas ambientales;
- la metrología y las técnicas de seguimiento;
- la interacción de los ecosistemas y la biodiversidad;
- el entorno ambiental (por ejemplo, aire, agua, suelo, fauna, flora);
- las técnicas para determinar el riesgo (por ejemplo, evaluación de aspectos/impactos ambientales, incluyendo los métodos para evaluar la significancia);
- el análisis del ciclo de vida;
- la evaluación del desempeño ambiental;
- la prevención y el control de la contaminación (por ejemplo, las mejores técnicas disponibles para el control de la contaminación o la eficiencia energética);
- la reducción de fuentes y las prácticas y los procesos para disminuir, reutilizar, reciclar y tratar los residuos.
- el uso de sustancias peligrosas;
- las emisiones de gases de efecto invernadero y su gestión;
- la gestión de los recursos naturales (por ejemplo, combustibles fósiles, agua, flora y fauna, suelo);
- el ecodiseño;
- la elaboración de informes ambientales y su comunicación;
- la responsabilidad extendida al producto;
- las tecnologías renovables y de bajas emisiones de carbono.

NOTA Para más información, véanse las normas relacionadas desarrolladas por el Comité Técnico ISO/TC 207 sobre gestión ambiental.

## A.4 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de la calidad

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— la terminología relacionada con la calidad, la gestión, la organización, el proceso y el producto, las características, la conformidad, la documentación, y los procesos de auditoría y de medición;

— el enfoque al cliente, los procesos relacionados con el cliente, el seguimiento y la medición de la satisfacción del cliente, el tratamiento de las quejas, el código de conducta, la resolución de conflictos;

— el liderazgo - función de la alta dirección, la gestión para el éxito sostenido de una organización – el enfoque a la gestión de la calidad, la obtención de beneficios financieros y económicos a través de la gestión de la calidad, los sistemas de gestión de la calidad y los modelos de excelencia;

— la participación de las personas, factores humanos, competencia, formación y toma de conciencia;

— el enfoque basado en procesos, análisis de procesos, capacidad y técnicas de control, métodos de tratamiento de riesgos;

— el enfoque de sistema para la gestión (base de los sistemas de gestión de la calidad, sistemas de gestión de la calidad y otros enfoques de sistemas de gestión, documentación del sistema de gestión de la calidad), tipos y valor, proyectos, planes de la calidad, gestión de la configuración;

— la mejora continua, innovación y aprendizaje;

— el enfoque basado en hechos para la toma de decisiones, técnicas de evaluación de riesgos (identificación de riesgos, análisis y evaluación), evaluación de la gestión de la calidad (auditoría, revisión y autoevaluación), técnicas de medición y seguimiento, requisitos para la medición de procesos y el equipo de medición, análisis de la causa raíz, técnicas estadísticas;

— las características de los procesos y los productos, incluyendo los servicios;

— las relaciones mutuamente beneficiosas con el proveedor, requisitos del sistema de gestión de la calidad y requisitos para los productos, requisitos particulares para la gestión de la calidad en diferentes sectores.

NOTA Para más información, véanse las normas relacionadas desarrolladas por el Comité Técnico ISO/TC 176 sobre gestión de la calidad.

## A.5 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de los registros

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— terminología relativa a los registros, los procesos de gestión de los registros y los sistemas de gestión de los registros;

— el desarrollo de medidas de desempeño y las métricas;

— la investigación y la evaluación de las prácticas relativas a registros a través de las entrevistas, la observación y la validación;

— el análisis de muestras de los registros creados en los procesos operacionales. Características clave de los registros, sistemas de registros, procesos y controles de los registros;

— la evaluación de riesgos (por ejemplo, la evaluación de riesgos a través de la imposibilidad de crear, mantener y controlar los registros adecuados de los procesos operacionales de la organización);

— el desempeño y la adecuación de los procesos de registros al crear, captar y controlar los registros;

— la evaluación de la adecuación y el desempeño de los sistemas de registros (incluyendo los sistemas operacionales para crear y controlar los registros), la idoneidad de las herramientas tecnológicas utilizadas y las instalaciones y los equipos establecidos;

— la evaluación de los diferentes niveles de competencia en la gestión de los registros requerida en una organización y la evaluación de esa competencia;

— la importancia del contenido, contexto, estructura, representación y control de la información (metadatos) requerida para definir y gestionar los registros y los sistemas de registros;

— los métodos para desarrollar instrumentos específicos de los registros;

— las tecnologías utilizadas para la creación, captura, conversión y migración, y la conservación a largo plazo de los registros electrónicos/digitales;

— la identificación e importancia de la documentación de autorización para los procesos de registro.

NOTA Para más información, véanse las normas relacionadas desarrolladas por el Subcomité Técnico ISO/TC 46/SC 11 sobre gestión de los registros.

## A.6 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de la resiliencia, la seguridad, el estado de preparación y la continuidad

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— los procesos, la ciencia y tecnología subyacentes a la gestión de la resiliencia, la seguridad, el estado de preparación, la respuesta, la continuidad y la recuperación;

— los métodos para la recopilación y el seguimiento de la información;

— la gestión del riesgo de sucesos perjudiciales (anticipar, evitar, impedir, proteger, mitigar, responder y recuperarse ante un suceso perjudicial);

— la evaluación del riesgo (identificación y valoración de activos; e identificación, análisis y evaluación del riesgo) y análisis de impacto (relacionado con los recursos humanos y materiales y los activos intangibles, así como el medio ambiente);

— el tratamiento de los riesgos (medidas adaptativas, proactivas y reactivas);

— los métodos y prácticas para la integridad y confidencialidad de la información;

— los métodos para la seguridad del personal y la protección de las personas;

— los métodos y prácticas para la protección de los bienes y la seguridad física;

— los métodos y prácticas para la prevención, la disuasión y la gestión de la seguridad;

— los métodos y prácticas para la mitigación de incidentes, la respuesta y la gestión de crisis;

— los métodos y prácticas para la gestión de la continuidad, la emergencia y la recuperación;

— los métodos y prácticas para el seguimiento, la medición y el informe sobre el desempeño (incluyendo las metodologías de prácticas y de pruebas).

NOTA Para más información, véanse las normas relacionadas desarrolladas por los Comités Técnicos ISO/TC 8, ISO/TC 223 e ISO/TC 247 sobre gestión de resiliencia, la seguridad, el estado de preparación y la continuidad.

## A.7 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de la seguridad de la información

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— las directrices de normas tales como ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005;

— la identificación y evaluación de los requisitos del cliente y de las partes interesadas;

— las leyes y reglamentos que tratan la seguridad de la información (por ejemplo, propiedad intelectual, contenido, protección y retención de los registros de la organización; protección y privacidad de datos; reglamentos de controles criptográficos; antiterrorismo; comercio electrónico; firma electrónica y digital; vigilancia en el puesto de trabajo; ergonomía del lugar de trabajo; intercepción de las telecomunicaciones y seguimiento de los datos (por ejemplo, correo electrónico), mal uso del equipo informático, recopilación de evidencias electrónicas, ensayos de vulnerabilidad, etc.;

— los procesos, la ciencia y la tecnología subyacentes a la gestión de la seguridad de la información;

— la evaluación del riesgo (identificación, análisis y evaluación) y tendencias en tecnología, amenazas y vulnerabilidades;

— la gestión del riesgo en la seguridad de la información;

— los métodos y las prácticas para los controles (electrónicos y físicos) de la seguridad de la información;

— los métodos y las prácticas para la integridad y confidencialidad de la información;

— los métodos y las prácticas para la medición y evaluación de la eficacia del sistema de gestión de la seguridad de la información y los controles asociados;

— los métodos y las prácticas para la medición, seguimiento y registro del desempeño (incluyendo pruebas, auditorías y revisiones).

NOTA Para más información, véanse las normas relacionadas desarrolladas por el Subcomité Técnico ISO/IEC JTC 1/SC 27 sobre gestión de la seguridad de la información.

## A.8 Ejemplo ilustrativo de conocimientos y habilidades de los auditores en la disciplina específica de gestión de la seguridad y salud en el trabajo

### A.8.1 Conocimientos y habilidades generales

Los conocimientos y habilidades relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos de la disciplina deberían ser los suficientes para permitir al auditor examinar el sistema de gestión y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

- la identificación de peligros, incluyendo los factores que afecten al desempeño humano en el lugar de trabajo (tales como factores físicos, químicos y biológicos, así como el género, la edad, la discapacidad u otros factores fisiológicos, psicológicos o de salud);
- la evaluación del riesgo, la determinación de controles y la comunicación de los riesgos [la determinación de controles debería basarse en la "jerarquía de los controles" (véase el apartado 4.3.1 de OHSAS 18001:2007)];
- la evaluación de factores de salud y factores humanos (incluyendo factores fisiológicos y psicológicos) y los principios para evaluarlos;
- los métodos de seguimiento de la exposición y de evaluación de los riesgos para la seguridad y salud en el trabajo (incluyendo aquellos que surjan de los factores humanos mencionados anteriormente o relacionados con la higiene en el trabajo) y de las estrategias relacionadas para eliminar o minimizar tales exposiciones;
- el comportamiento humano, las interacciones entre personas y la interacción entre personas y máquinas, los procesos y el entorno de trabajo (incluido el lugar de trabajo, los principios de ergonomía y de diseño seguro, las tecnologías de la información y la comunicación);
- la evaluación de los diferentes tipos y niveles de competencia en materia de seguridad y salud en el trabajo requerida en una organización y la evaluación de esas competencias;
- los métodos para fomentar la participación e implicación de los empleados;
- los métodos para fomentar el bienestar y la responsabilidad personal del empleado (en relación con el tabaco, las drogas, el alcohol, las cuestiones relacionadas con el peso, el ejercicio, el estrés, el comportamiento agresivo, etc.), tanto durante el horario laboral como en su vida privada;
- el desarrollo, uso y evaluación de las medidas del desempeño proactivas y reactivas y las métricas;
- los principios y prácticas para identificar las situaciones de emergencia potenciales y la planificación, prevención, respuesta y recuperación en caso de emergencia;
- los métodos para la investigación y evaluación de incidentes (incluyendo los accidentes y las enfermedades laborales);
- la determinación y el uso de información relacionada con la salud (incluyendo el seguimiento de los datos relativos a la exposición en el trabajo y de enfermedad) – pero prestando especial consideración a la confidencialidad sobre aspectos particulares de tal información;
- la comprensión de la información médica (incluyendo la terminología médica suficiente para comprender los datos relacionados con la prevención de lesiones y la mala salud);
- los sistemas de valores límite de exposición en el trabajo;
- los métodos para el seguimiento y la elaboración de informes sobre el desempeño de la seguridad y salud en el trabajo;
- la comprensión de los requisitos legales y otros requisitos pertinentes para la seguridad y salud en el trabajo, suficientes para permitir al auditor evaluar el sistema de gestión de la seguridad y salud en el trabajo.

### A.8.2 Conocimientos y habilidades relacionados con el sector que se audita

Los conocimientos y las habilidades relacionados con el sector que se audita deberían ser los suficientes para permitir al auditor examinar el sistema de gestión dentro del contexto del sector y generar los hallazgos y conclusiones de la auditoría apropiados.

Son ejemplos:

— los procesos, equipos, materias primas, sustancias peligrosas, ciclos de proceso, mantenimiento, logística, organización del flujo de trabajo, prácticas de trabajo, planificación de turnos, cultura de la organización, liderazgo, comportamiento y otras cuestiones específicas de la operación o el sector;

— los peligros y riesgos típicos, incluyendo factores de salud y factores humanos, para el sector.

NOTA Para más información, véanse las normas relacionadas desarrolladas por el grupo de proyecto OHSAS sobre gestión de la seguridad y salud en el trabajo.

# Anexo B
(informativo)

# Orientación adicional destinada a los auditores para planificar y realizar las auditorías

## B.1 Aplicación de los métodos de auditoría

Una auditoría puede realizarse usando una variedad de métodos de auditoría. En este Anexo puede encontrarse una explicación de los métodos de auditoría usados comúnmente. Los métodos de auditoría elegidos para una auditoría dependen de los objetivos de la auditoría, el alcance y los criterios definidos, así como de la duración y la ubicación. También deberían considerarse la competencia disponible de los auditores y cualquier duda que surja de la aplicación de los métodos de auditoría. Aplicar una variedad y combinación de diferentes métodos de auditoría puede optimizar la eficiencia y eficacia del proceso de auditoría y sus resultados.

La realización de una auditoría implica una interacción entre individuos con el sistema de gestión que se audita y la tecnología utilizada para llevar a cabo la auditoría. La Tabla B.1 proporciona ejemplos de métodos de auditoría que pueden usarse, por separado o en combinación, para alcanzar los objetivos de la auditoría. Si una auditoría supone el uso de un equipo auditor con múltiples miembros, pueden usarse métodos in situ y métodos a distancia simultáneamente.

NOTA Se proporciona información adicional sobre las visitas in situ en el capítulo B.6.

**Tabla B.1 – Métodos de auditoría aplicables**

| Grado de implicación entre el auditor y el auditado | Ubicación del auditor | |
|---|---|---|
| | **In situ** | **A distancia** |
| **Interacción humana** | Realizar entrevistas.<br>Completar listas de verificación y cuestionarios con la participación del auditado.<br>Revisar los documentos con la participación del auditado.<br>Muestrear. | A través de medios de comunicación interactivos:<br>— realizar entrevistas;<br>— completar listas de verificación y cuestionarios;<br>— revisar los documentos con la participación del auditado. |
| **Sin interacción humana** | Revisar los documentos (por ejemplo, registros, análisis de datos).<br>Observar el trabajo desempeñado.<br>Realizar visitas al sitio.<br>Completar listas de verificación.<br>Muestrear (por ejemplo, productos). | Revisar los documentos (por ejemplo, registros, análisis de datos).<br>Observar el trabajo desempeñado a través de medios de vigilancia, considerando los requisitos sociales y legales.<br>Analizar los datos. |
| Las actividades de auditoría in situ se realizan en las instalaciones del auditado. Las actividades de auditoría a distancia se realizan en cualquier otro lugar distinto de las instalaciones del auditado, sin tener en cuenta la distancia.<br>Las actividades de auditoría interactivas implican la interacción entre el personal del auditado y el equipo auditor. Las actividades de auditoría no interactivas no implican la interacción humana con las personas que representan al auditado, pero implican la interacción con los equipos, las instalaciones y la documentación. | | |

La responsabilidad de la aplicación eficaz de los métodos de auditoría para cualquier auditoría dada en la etapa de planificación recae en la persona responsable de gestionar el programa de auditoría o en el líder del equipo auditor. El líder del equipo auditor es responsable de realizar las actividades de auditoría.

La viabilidad de las actividades de auditoría a distancia puede depender del nivel de confianza que existe entre el auditor y el personal del auditado.

En lo que respecta al programa de auditoría, debería asegurarse que el uso de la aplicación a distancia e in situ de los métodos de auditoría es adecuado y equilibrado, para asegurar el logro satisfactorio de los objetivos del programa de auditoría.

## B.2 Realización de la revisión de los documentos

Los auditores deberían considerar si:

— la información contenida en los documentos proporcionados es:

  — completa (todo el contenido esperado está en el documento);

  — correcta (el contenido es conforme con otras fuentes fiables, tales como normas y reglamentos);

  — coherente (el documento es coherente consigo mismo y con documentos relacionados);

  — actual (el contenido está actualizado);

— los documentos que están siendo revisados cubren el alcance de la auditoría y proporcionan información suficiente para apoyar los objetivos de la auditoría;

— el uso de tecnologías de la información y las comunicaciones, dependiendo de los métodos de auditoría, promueve la realización eficiente de la auditoría. Se necesita un cuidado específico para la seguridad de la información debido a los reglamentos aplicables sobre protección de datos (en particular para la información que queda fuera del alcance de la auditoría pero que también está contenida en el documento).

NOTA La revisión de los documentos puede dar una indicación de la eficacia del control de los documentos dentro del sistema de gestión del auditado.

## B.3 Muestreo

### B.3.1 Generalidades

El muestreo para la auditoría tiene lugar cuando no es práctico o no es rentable examinar toda la información disponible durante la auditoría, por ejemplo, los registros son demasiado numerosos o están demasiado dispersos geográficamente para justificar el examen de cada elemento de la población. El muestreo para la auditoría de una población grande es el proceso de seleccionar menos del 100% de los elementos dentro del conjunto total de datos disponibles (población) para obtener y evaluar la evidencia sobre alguna característica de esa población, para formar una conclusión sobre la población.

El objetivo del muestreo de la auditoría es proporcionar información para que el auditor tenga confianza en que los objetivos de la auditoría pueden alcanzarse o se alcanzarán.

El riesgo asociado con el muestreo es que las muestras pueden no ser representativas de la población de la que se seleccionan, y por tanto la conclusión del auditor puede estar sesgada y ser diferente de la que se alcanzaría si se examinara toda la población. Puede haber otros riesgos dependiendo de la variabilidad dentro de la población de la que se va a realizar el muestreo y del método elegido.

El muestreo para la auditoría generalmente implica los siguientes pasos:

— establecer los objetivos del plan de muestreo;

— seleccionar la extensión y la composición de la población de la que se va a realizar el muestreo;

— seleccionar un método de muestreo;

— determinar el tamaño de la muestra a tomar;

— llevar a cabo la actividad de muestreo;

— recopilar, evaluar, informar y documentar los resultados.

Al realizar el muestreo, debería considerarse la calidad de los datos disponibles, ya que un muestreo de datos insuficientes o imprecisos no dará un resultado útil. La selección de una muestra apropiada debería basarse en el método de muestreo y en el tipo de datos requeridos, por ejemplo, para inferir un patrón de comportamiento particular o realizar inferencias sobre una población.

El informe de la muestra seleccionada podría tener en cuenta el tamaño de la muestra, el método de selección y las estimaciones hechas basadas en la muestra y el nivel de confianza.

Las auditorías pueden utilizar muestreos basados en juicios (véase B.3.2) o muestreos estadísticos (véase B.3.3).

### B.3.2 Muestreo basado en juicios

El muestreo basado en juicios depende de los conocimientos, habilidades y experiencia del equipo auditor (véase el capítulo 7).

Para el muestreo basado en juicios puede considerarse lo siguiente:

— la experiencia de auditorías previas dentro del alcance de la auditoría;

— la complejidad de los requisitos (incluyendo los requisitos legales) para alcanzar los objetivos de la auditoría;

— la complejidad e interacción de los procesos de la organización y los elementos del sistema de gestión;

— el grado de cambio en la tecnología, el factor humano o el sistema de gestión;

— las áreas clave de riesgo previamente identificadas y las áreas de mejora;

— el resultado del seguimiento de los sistemas de gestión.

Un inconveniente del muestreo basado en juicios es que puede no haber una estimación estadística del efecto de la incertidumbre en los hallazgos de la auditoría y en las conclusiones alcanzadas.

### B.3.3 Muestreo estadístico

Si se decide utilizar muestreo estadístico, el plan de muestreo debería basarse en los objetivos de la auditoría y en lo que se conoce sobre las características de la población global de la que se toman las muestras.

— El diseño del muestreo estadístico utiliza un proceso de selección de la muestra basado en la teoría de la probabilidad. El muestreo basado en atributos se usa cuando sólo hay dos posibles resultados muestrales para cada muestra (por ejemplo, correcto/incorrecto o apto/no apto). El muestreo basado en variables se utiliza cuando el resultado de la muestra se da en un rango continuo.

— El plan de muestreo debería tener en cuenta si es probable que los resultados que se examinan estén basados en atributos o basados en variables. Por ejemplo, cuando se evalúa la conformidad de los formularios completados con los requisitos establecidos en un procedimiento, podría usarse un enfoque basado en atributos. Cuando se examina la ocurrencia de incidentes de seguridad alimentaria o el número de infracciones de seguridad, es probable que sea más apropiado un enfoque basado en variables.

— Los elementos clave que afectarán al muestreo de la auditoría son:

  — el tamaño de la organización;

  — el número de auditores competentes;

  — la frecuencia de auditorías en el curso del año;

  — la duración de la auditoría individual;

  — cualquier nivel de confianza requerido externamente.

— Cuando se desarrolla un plan de muestreo estadístico, el nivel de riesgo muestral que el auditor está dispuesto a aceptar es una consideración importante. A veces esto se denomina nivel de confianza aceptable. Por ejemplo, un riesgo muestral del 5% corresponde a un nivel de confianza aceptable del 95%. Un riesgo muestral del 5% significa que el auditor está dispuesto a aceptar el riesgo de que 5 de cada 100 (o 1 de cada 20) de las muestras examinadas no reflejará los valores reales que se verían si se examinara toda la población.

— Cuando se utiliza el muestreo estadístico, los auditores deberían documentar apropiadamente el trabajo realizado. Esto debería incluir una descripción de la población que se pretende muestrear, los criterios muestrales utilizados para la evaluación (por ejemplo, qué es una muestra aceptable), los parámetros estadísticos y los métodos que se utilizaron, el número de muestras evaluadas y los resultados obtenidos.

## B.4 Preparación de los documentos de trabajo

Al preparar los documentos de trabajo, el equipo auditor debería considerar las siguientes preguntas para cada documento:

a) ¿Qué registro de auditoría se creará utilizando este documento de trabajo?

b) ¿A qué actividad de la auditoría afecta este documento de trabajo en particular?

c) ¿Quién será el usuario de este documento de trabajo?

d) ¿Qué información se necesita para preparar este documento de trabajo?

Para las auditorías combinadas, deberían desarrollarse documentos de trabajo para evitar la duplicación de actividades de auditoría mediante:

— la agrupación de requisitos similares provenientes de criterios diferentes;

— la coordinación del contenido de listas de verificación y cuestionarios relacionados.

Los documentos de trabajo deberían ser adecuados para tratar todos aquellos elementos del sistema de gestión dentro del alcance de la auditoría y pueden facilitarse en cualquier medio.

## B.5 Selección de las fuentes de información

Las fuentes de información seleccionadas pueden variar de acuerdo con el alcance y la complejidad de la auditoría y pueden incluir lo siguiente:

— entrevistas con empleados y con otras personas;

— observación de actividades y el ambiente de trabajo y condiciones circundantes;

— documentos, tales como políticas, objetivos, planes, procedimientos, normas, instrucciones, licencias y permisos, especificaciones, planos, contratos y pedidos;

— registros, tales como registros de inspección, actas de reuniones, informes de auditoría, registros de programas de seguimiento y resultados de mediciones;

— resúmenes de datos, análisis e indicadores de desempeño;

— información sobre los programas de muestreo del auditado y sobre los procedimientos para el control de los procesos de muestreo y medición;

— informes de otras fuentes, por ejemplo, retroalimentación del cliente, encuestas y mediciones externas, otra información pertinente de partes externas y la calificación de los proveedores;

— bases de datos y sitios en Internet;

— simulaciones y modelizaciones.

## B.6 Orientación sobre la visita a la ubicación del auditado

Para minimizar la interferencia entre las actividades de auditoría y los procesos de trabajo del auditado y para asegurar la salud y la seguridad del equipo auditor durante la visita, debería considerarse lo siguiente:

a) planificar la visita:

- — asegurar la autorización y el acceso a aquellas partes de la ubicación del auditado, para visitarlas de acuerdo con el alcance de la auditoría;
- — proporcionar la información adecuada (por ejemplo, reunión informativa) a los auditores sobre seguridad, salud (por ejemplo, cuarentena), cuestiones de seguridad y salud en el trabajo y normas culturales para la visita, incluyendo la vacunación y autorizaciones requeridas y recomendadas, si es aplicable;
- — confirmar con el auditado que cualquier equipo de protección individual estará disponible para el equipo auditor, si es aplicable;
- — excepto para auditorías ad hoc no programadas, asegurarse de que el personal visitado será informado sobre los objetivos y el alcance de la auditoría;

b) actividades in situ:

- — evitar cualquier interrupción innecesaria de los procesos operativos;
- — asegurarse de que el equipo auditor está utilizando el equipo de protección individual correctamente;
- — asegurarse de que se comunican los procedimientos de emergencia (por ejemplo, salidas de emergencia, puntos de reunión);
- — programar la comunicación para minimizar las interrupciones;
- — adaptar el tamaño del equipo auditor y el número de guías y observadores de acuerdo con el alcance de la auditoría, para evitar interferencias con los procesos operativos tanto como sea posible;
- — no tocar ni manipular ningún equipo, a menos que se permita explícitamente, incluso cuando se tenga la competencia o se esté autorizado;

- si tiene lugar un incidente durante la visita in situ, el líder del equipo auditor debería revisar la situación con el auditado y, si es necesario, con el cliente de la auditoría y llegar a un acuerdo sobre si la auditoría debería interrumpirse, volver a programarse o continuar;
- si se toman fotografías o material de vídeo, pedir la autorización de la dirección con antelación y considerar las cuestiones de seguridad y confidencialidad, y evitar tomar fotografías de personas sin su permiso;
- si se hacen copias de documentos de cualquier tipo, pedir permiso con antelación y considerar las cuestiones de confidencialidad y seguridad;
- cuando se toman notas, evitar recopilar información personal a menos que lo requieran los objetivos de la auditoría o los criterios de auditoría.

## B.7 Realización de entrevistas

Las entrevistas son uno de los medios importantes de recopilar información y deberían llevarse a cabo de un modo adaptado a la situación y a la persona entrevistada, sea cara a cara o por otros medios de comunicación. Sin embargo, el auditor debería considerar lo siguiente:

- las entrevistas deberían mantenerse con personas de los niveles y funciones apropiados que desempeñan actividades o tareas dentro del alcance de la auditoría;
- las entrevistas normalmente deberían llevarse a cabo durante la jornada de trabajo normal y, cuando sea posible, en el lugar de trabajo normal de la persona entrevistada;
- intentar que la persona entrevistada esté a gusto antes de la entrevista y durante la misma;
- debería explicarse la razón de la entrevista y cualquier toma de notas;
- las entrevistas pueden iniciarse preguntando a las personas que describan su trabajo;
- selección cuidadosa del tipo de pregunta utilizado (por ejemplo, preguntas abiertas, cerradas, inductivas);
- los resultados de la entrevista deberían resumirse y revisarse con la persona entrevistada;
- debería agradecerse a las personas entrevistadas su participación y cooperación.

## B.8 Hallazgos de la auditoría

### B.8.1 Determinación de los hallazgos de la auditoría

Al determinar los hallazgos de la auditoría, debería considerarse lo siguiente:

- el seguimiento de los registros y las conclusiones de auditorías previas;
- los requisitos del cliente de la auditoría;
- los hallazgos que excedan la práctica normal, o las oportunidades de mejora;
- el tamaño muestral;
- la categorización (si la hay) de los hallazgos de la auditoría;

### B.8.2 Registro de conformidades

Para los registros de conformidad, debería considerarse lo siguiente:

— la identificación de los criterios de auditoría respecto a los que se muestra la conformidad;

— la evidencia de la auditoría para respaldar la conformidad;

— la declaración de conformidad, si es aplicable.

### B.8.3 Registro de no conformidades

Para los registros de las no conformidades, debería considerarse lo siguiente:

— la descripción de los criterios de auditoría o la referencia a los mismos;

— la declaración de no conformidad;

— la evidencia de la auditoría;

— los hallazgos de la auditoría relacionados, si es aplicable.

### B.8.4 Tratamiento de los hallazgos relacionados con múltiples criterios

Durante una auditoría es posible identificar hallazgos relacionados con múltiples criterios. Cuando un auditor identifica un hallazgo vinculado a un criterio o una auditoría combinada, el auditor debería considerar el posible impacto en los criterios correspondientes o similares de los otros sistemas de gestión.

Dependiendo de lo acordado con el cliente de la auditoría, el auditor puede considerar:

— hallazgos separados para cada criterio; o

— un único hallazgo, combinando las referencias a los múltiples criterios.

Dependiendo de lo acordado con el cliente de la auditoría, el auditor puede guiar al auditado sobre cómo responder a esos hallazgos.

# Bibliografía


[1] ISO 2859-4, *Sampling procedures for inspection by attributes — Part 4: Procedures for assessment of declared quality levels*

[2] ISO 9000:2005, *Sistemas de gestión de la calidad — Fundamentos y vocabulario*

[3] ISO 9001, *Sistemas de gestión de la calidad — Requisitos*

[4] ISO 14001, *Sistemas de gestión ambiental — Requisitos con orientación para su uso*

[5] ISO 14050, *Gestión ambiental — Vocabulario*

[6] ISO/IEC 17021:2011, *Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión*

[7] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[8] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

[9] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

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

[12] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[13] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

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

[15] ISO 28000, *Specification for security management systems for the supply chain*

[16] ISO 30301[1)], *Information and documentation — Management system for records — Requirements*

[17] ISO 31000, *Risk management — Principles and guidelines*

[18] ISO 39001[2)], *Road traffic safety (RTS) management systems — Requirements with guidance for use*

[19] ISO 50001, *Sistemas de gestión de la energía — Requisitos con orientación para su uso*

[20] ISO Guide 73:2009, *Risk management — Vocabulary*


---

1) Pendiente de publicación.

2) En preparación.

[21] OHSAS 18001:2007, *Occupational health and safety management systems — Requirements*

[22] Documentos del *ISO 9001 Auditing Practices Group* disponibles en:
www.iso.org/tc176/ISO9001AuditingPracticesGroup

[23] Directrices adicionales sobre la Norma ISO 19011[2)] disponibles en:
www.iso.org/19011auditing

**ICS 03.120.10; 13.020.10**
Precio basado en 44 páginas