NORMA INTERNACIONAL **ISO 19011**

Segunda edición
2011-11-15

Directrices para la auditoría de Sistemas de Gestión

Número de Referencia
ISO 19011:2011 (E)

DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org
Publicado en Suiza

Índice

Page

Prólogo

ISO (la 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 (CEI) en todas las materias de normalización electrotécnica.

Las Normas Internacionales se redactan de acuerdo con las reglas establecidas en la Parte 3 de las Directivas ISO/CEI.

La tarea principal de los comités técnicos es preparar Normas Internacionales. Los Proyectos de Normas Internacionales aceptados por los comités técnicos son enviados a los organismos miembros para votación. La publicación como Norma Internacional requiere la aprobación por al menos el 75% de los organismos miembros requeridos para votar.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta Norma Internacional 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 fue preparada por el Comité Técnico ISO/TC 176, *Gestión Aseguramiento de la Calidad* y el Subcomité SC 3, *Tecnologías de Apoyo*.

Esta segunda edición cancela y reemplaza la primera edición (ISO 19011:2002), la cual ha sido revisada técnicamente.

Las principales diferencias comparada con la primera edición son:

— Se ha ampliado el alcance de auditoría a sistemas de gestión de calidad y ambiental a la auditoría de cualquier sistema de gestión;
— Se ha aclarado la relación entre ISO 19011 e ISO/IEC 17021;
— Se han introducido métodos remotos de auditoría y el concepto de riesgo;
— Se ha adicionado la confidencialidad a los principios de auditoría;
— Las cláusulas 5, 6 y 7 han sido reorganizadas;
— Se ha incluido información adicional en un Nuevo Anexo B, lo que dio como resultado la remoción de las cajas de ayuda;
— Los procesos de determinación de competencias y de evaluación han sido fortalecidos;
— Se han incluido ejemplos ilustrativos de conocimiento específico de disciplina y otras habilidades en el Nuevo anexo A;
— Lineamientos adicionales están disponibles en la siguiente dirección: www.iso.org/19011auditing.

Introducción

Desde la publicación de la primera edición de esta Norma Internacional en 2002, se han publicado un gran número de normas para sistemas de gestión. Por lo tanto, existe ahora la necesidad de considerar un alcance más amplio para la auditoría de sistemas de gestión, así como de proveer lineamientos más generales.

En 2006, el Comité ISO, por evaluación de conformidad (CASCO) desarrolló ISO/IEC 17021, que establece los requisitos para la certificación de sistemas de gestión y que en parte se basó en los lineamientos contenidos en la primera edición de esta Norma Internacional.

La segunda edición de ISO/IEC 17021, publicada en 2011, se extendió de manera tal que transformó los lineamientos ofrecidos 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 provee guía para todos los usuarios, incluyendo organizaciones pequeñas y medianas y se concentra en lo que se conoce comúnmente como “auditorías internas” (de primera parte) y “auditorías conducidas por parte de los clientes sobre sus proveedores” (de segunda parte). Mientras que aquellos involucrados en auditorías de certificación de sistemas de gestión siguen los requisitos de ISO/IEC 17021:2011, y pueden hallar útil también los lineamientos contenidos en esta Norma Internacional.

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

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

Auditoría Interna	Auditoría Externa	
	Auditoría a proveedores	**Auditorías de 3ra parte**
A veces llamada auditoría de primera parte.	A veces llamada auditoría de segunda parte.	Para propósitos legales, regulatorios y similares. Para certificación (ver también los requisitos en ISO/IEC 17021:2011)

Esta Norma Internacional no establece requisitos, sino que provee una guía sobre el manejo de un programa de auditoría, sobre la planeación y realización de una auditoría a un sistema de gestión, así como sobre la competencia y evaluación de un auditor que pertenezca al equipo auditor.

Las organizaciones pueden tener y operar más de un sistema de gestión formal. Para simplificar la lectura de esta Norma Internacional, se preferirá la forma singular de “Sistema de Gestión”, pero el lector puede adaptar la implementación de la guía a su propia situación particular. Esto también aplica para el uso de “persona” y “personas”, “auditor” y “auditores”.

Se busca que esta Norma Internacional sea aplicable a un amplio rango de usuarios potenciales, incluyendo auditores, organizaciones que están implementando sistemas de gestión, y organizaciones que necesitan realizar auditorías a sus sistemas de gestión por razones contractuales o regulatorias. Los usuarios de esta Norma Internacional pueden sin embargo, aplicar esta guía durante el desarrollo de sus propios requisitos de auditoría.

La guía contenida en esta Norma Internacional también puede ser usada con el propósito de auto-declaración y puede resultar útil a organizaciones involucradas en entrenamiento de auditores o certificación de personal.

Se busca que la guía contenida en esta Norma Internacional sea flexible. Tal como se indica en varios puntos de este texto, el uso de esta guía puede diferir dependiendo del tamaño y nivel de madurez del sistema de gestión de una organización y de la naturaleza y complejidad de la organización a ser auditada, así como de los objetivos y alcance de las auditorías a realizar.

Esta Norma Internacional introduce el concepto de riesgo a la auditoría de sistemas de gestión. El enfoque adoptado relaciona tanto el riesgo de que el proceso de auditoría no alcance sus objetivos como el potencial de que la auditoría interfiera con las actividades y procesos de los auditados. Esta no provee lineamientos específicos sobre le proceso de gestión de riesgo de la organización, pero reconoce que las organizaciones pueden enfocar los esfuerzos de auditoría en temas que sean significativos a los sistemas de gestión.

Esta Norma Internacional adopta el término “auditoría combinada” para aquellos casos en que se auditan dos o más sistemas de gestión de diferentes disciplinas. Cuando estos sistemas están integrados a un único sistema de gestión, los procesos de auditoría son los mismos que para una auditoría combinada.

El Capítulo 3 establece los términos y definiciones claves usadas en esta Norma Internacional. Se han hecho todos los esfuerzos para asegurar que estas definiciones no entran en conflicto con las definiciones usadas en otras normas.

El Capítulo 4 describe los principios en los que se basa la auditoría. Estos principios ayudan a los usuarios a entender la naturaleza esencial de la auditoría y resultan importantes para entender la guía presentada en los Capítulos 5 y 7.

El Capítulo 5 provee lineamientos sobre el establecimiento y manejo de un programa de auditoría, estableciendo los objetivos del programa y coordinando las actividades de auditoría.

El Capítulo 6 provee guías sobre la planeación y realización de una auditoría a un sistema de gestión.

El Capítulo 7 provee lineamientos relacionados con la competencia y evaluación de los auditores de sistemas de gestión y de los equipos de auditoría.

El Anexo A ilustra la aplicación de las guías que aparecen en el Capítulo 7 para diferentes disciplinas.

El Anexo B provee lineamientos adicionales para auditores sobre la planeación y realización de auditorías.

Directrices para auditoría de sistemas de gestión

1 Alcance

Esta Norma Internacional proporciona directrices sobre la auditoría a sistemas de gestión, incluyendo los principios de auditoría, el manejo de un programa de auditoría y la realización de las auditorías a sistemas de gestión, así como directrices sobre la evaluación de competencia de los individuos involucrados en el proceso de auditoría, incluyendo el personal que maneja el programa de auditoría, los auditores y los equipos de auditoría.

Esta es aplicable a todas las organizaciones que requieren llevar a cabo auditorías internas o externas a sistemas de gestión o manejar un programa de auditoría.

La aplicación de esta Norma Internacional a otros tipos de auditoría es posible, en tanto se de consideración especial a la competencia específica requerida.

2 Referencias Normativas

No se citan referencias normativas. Esta cláusula se incluye con el fin de mantener la misma numeración de cláusulas de otras normas ISO de sistemas de gestión.

3 Términos y Definiciones

Para los propósitos de este documento, 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 la extensión en que se cumplen los criterios de auditoría (3.2).

NOTA 1 Las auditorías internas, denominadas en algunos casos como auditorías de primera parte, se realizan por, o en nombre de, la propia organización, para la revisión por la dirección y con otros fines internos (ej. para confirmar la efectividad del sistema de gestión o para obtener información para la mejora del sistema de gestión). Las auditorías internas pueden constituir la base para la autodelcaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar el auditor libre de responsabilidad de la actividad que se audita o libre de prejuicios o conflicto de intereses.

NOTA 2 Las auditorías externas incluyen lo que se denomina generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes y externas, tales como aquellas que proporcionan el registro o la certificación de conformidad.

NOTE 3 Cuando se auditan juntos dos o más sistemas de gestión de diferentes disciplinas (ej. calidad, ambiental, seguridad y salud ocupacional), esto se denomina auditoría combinada.

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

NOTE 5 Adaptado de ISO 9000:2005, definición 3.9.1.

3.2
Criterios de auditoría
Grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la **evidencia de auditoría** (3.3)

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

NOTA 2 si los criterios de auditoría son legales, se utilizan a menudo los términos “cumple” o “no cumple” en un **hallazgo de auditoría** (3.4).

3.3
evidencia de la auditoría
Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría (3.2) y que son verificables.

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 auditoría indican conformidad o no conformidad.

NOTA 2 Los hallazgos de auditoría pueden llevar a la identificación de oportunidades de mejora o al registro de mejores prácticas.

NOTA 3 Si los criterios de auditoría son seleccionados de requisitos legales o de otra índole, los hallazgos de auditoría se denominan Cumplimiento o Incumplimiento.

NOTA 4 Adaptado de 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 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 auditoría también puede ser el **auditado** (3.7) o la persona que maneja el programa de auditoría. La solicitud de auditoría externa pude venir de diferentes fuentes tales como entes reguladores, partes contratantes o clientes potenciales.

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

3.7
auditado
organización que está siendo 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 auditor 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 no audita

NOTA 1 Un observador no es parte del **equipo auditor** (3.9) y no influencia o interfiere con la realización de la **auditoría** (3.1).

NOTA 2 Un observador pude ser una persona del **auditado** (3.7), un regulador u otra parte interesada que fue testigo de la **auditoría** (3.1).

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

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

NOTA Adaptado de 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 período 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 en los objetivos

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

3.17
competencia
habilidad para aplicar conocimientos y habilidades para alcanzar los resultados esperados

NOTA Habilidad implica la aplicación apropiada de 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 políticas y objetivos y para alcanzar dichos objetivos

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

[ISO 9000:2005, definición 3.2.2]

4 Principios de auditoría

La auditoria se caracteriza por depender de varios principios. Éstos deberían 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 trabajar independientemente entre sí para alcanzar conclusiones similares en circunstancias similares.

Los lineamientos dados en los Capítulos 5 a 7 están basados en los siguientes principios:

a) **Integridad**: el fundamento del profesionalismo

Los auditores y la persona que maneja el programa de auditoría deberían:
- — llevar a cabo su trabajo con honestidad, diligencia y responsabilidad;
- — observar y cumplir con todos los requisitos legales aplicables;
- — demostrar su competencia durante el desarrollo del trabajo;
- — llevar a cabo su trabajo de manera imparcial; es decir, ser justo e imparcial en todos sus negocios;
- — ser sensible a cualquier influencia ejercida sobre su juicio durante el curso de una auditoría.

b) **Presentación ecuánime**: obligación de reportar con veracidad y exactitud

Los hallazgos, conclusiones e informes de la auditoría deberían reflejar con veracidad y exactitud las actividades de la auditoría. Se informa 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 sincera, exacta, objetiva, clara y complete.

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 en el desempeño de su trabajo con el debido cuidado profesional es tener la habilidad de hacer juicios razonables en toda situación de auditoría.

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

Los auditores deberían ejercitar la discreción en el uso y protección de la información adquirida en el curso de sus labores. La información de auditoría no debería ser usada de manera inapropiada para ganancia personal del auditor o del cliente de auditoría ni de manera tal que vaya en detrimento de los intereses legítimos del auditado. Este concepto incluye el adecuado manejo de información confidencial sensible.

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 es auditada mientras esto sea posible, y en todo caso actuarán de manera tal que estén libres de sesgo y conflicto de intereses. Para auditorías internas, los auditores deberían ser independientes de los gerentes operativos de las funciones a ser auditadas. Los auditores deberían mantener una actitud objetiva 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 organizaciones pequeñas, es posible que los auditores no puedan ser completamente independientes de la actividad a auditor, pero se debería hacer todo esfuerzo para quitar los sesgos y animar la objetividad.

f) **Enfoque basado en la evidencia:** el método racional para alcanzar conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático

La evidencia de la auditoría debería ser verificable. En general, está basada en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un período de tiempo delimitado y con recursos finitos. Se debería aplicar un uso adecuado del muestreo, ya que éste 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 una auditoría debería establecer un programa de auditoría que contribuya a la determinación de la efectividad del sistema de gestión del auditado. El programa de auditoría puede incluir auditorías que tengan en cuenta una o más normas de sistemas de gestión ya sean llevadas a cabo por separado o en combinación.

La alta gerencia debería asegurar que los objetivos del programa de auditoría se hayan establecido y asignar una o más personas competentes para gestionar el programa de auditoría. El alcance de un programa de auditoría debería estar basado en el tamaño y naturaleza de la organización a ser auditada, así como en la naturaleza, funcionalidad y complejidad y el nivel de madurez del sistema de gestión que se va a auditar. Se debería dar prioridad a asignar los recursos del programa de auditoría para auditar aquellos temas de mayor significancia dentro del sistema de gestión. Estos pueden incluir las características clave de calidad del producto o los peligros relacionados a salud y seguridad o aspectos ambientales significativos y su control.

NOTA Este concepto es comúnmente conocido como auditoría basada en riesgos. Esta Norma Internacional no da lineamientos adicionales para auditorías basadas en riesgos.

El programa de auditoría debería incluir la información y recursos necesarios para organizar y conducir las auditorías de manera eficiente dentro de los tiempos especificados y también puede incluir lo siguiente:

— objetivos para el programa de auditoría y auditorías individuales;
— alcance/número/tipos/duración/ubicación/cronograma de las auditorías;
— procedimientos del programa de auditoría;
— criterios de auditoría;
— métodos de auditoría;
— selección de equipos auditores;
— recursos necesarios, incluyendo viajes y hospedaje;
— procesos para manejo de confidencialidad, seguridad de la información, salud y seguridad y otros temas similares.

La implementación del programa de auditoría debería ser monitoreado y medido para asegurar que se han alcanzado los objetivos trazados. El programa de auditoría debería ser revisado para identificar posibles mejoras.

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

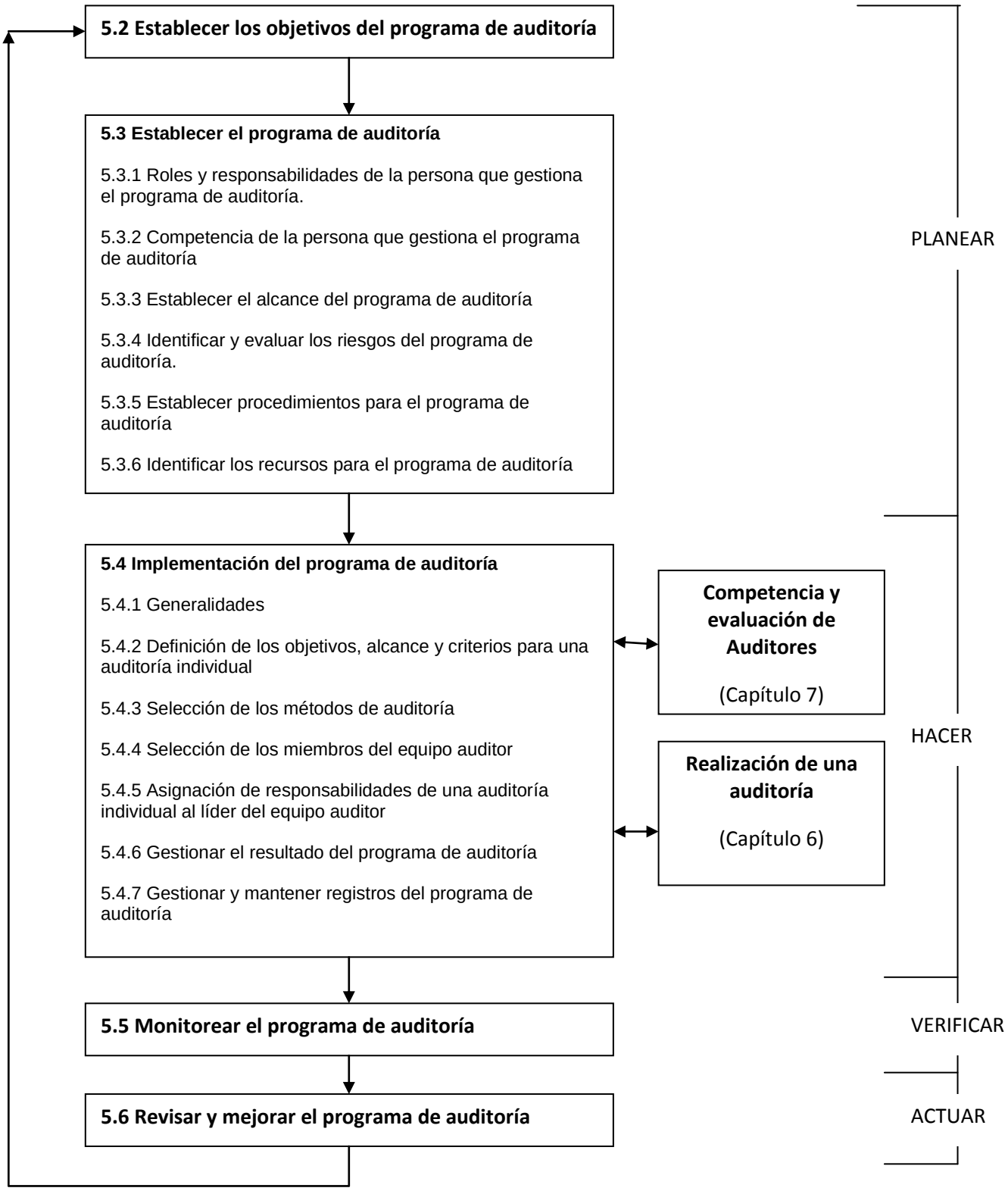


Figura 1 —Diagrama de flujo del proceso para la gestión de un programa de auditoría

NOTA 1 Esta figura también ilustra la aplicación de la metodología Planificar-Hacer-Verificar-Actuar en esta Norma Internacional.

NOTA 2 Los números en ésta y en todas las figuras subsiguientes hacen referencia a los capítulos pertinentes de esta Norma Internacional.

5.2 Establecer los objetivos del programa de auditoría

La alta gerencia debería asegurar que se hayan establecido los objetivos del programa de auditoría de manera tal que sirvan para dirigir la planeación de las auditorías y para conducirlas y debería asegurar que el programa de auditoría está efectivamente implementado. Los objetivos del programa de auditoría deberían ser consistentes con y deberían soportar la política y objetivos del sistema.

Estos objetivos pueden estar basados en consideración a lo siguiente:

a) prioridades de la gerencia;
b) intenciones comerciales y de otros negocios;
c) características de procesos, productos y proyectos y cualquier cambio en estos;
d) requisitos del sistema de gestión;
e) requisitos legales y contractuales y otros requisitos a los que la organización esté comprometida;
f) necesidad de evaluación de proveedor;
g) necesidades y expectativas de las partes interesadas, incluyendo clientes;
h) nivel de desempeño del auditado, reflejado en la ocurrencia de fallas o incidentes o quejas de clientes;
i) riesgos para el auditado;
j) resultados de auditorías previas;
k) nivel de madurez del sistema de gestión a ser auditado.

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

— contribuir con la mejora del sistema de gestión y su desempeño;
— cumplir con requisitos externos, ej. Certificación de una norma de sistema de gestión;
— verificar conformidad con requisitos contractuales;
— obtener y mantener confianza en la capacidad de un proveedor;
— determinar la efectividad del sistema de gestión;
— evaluar la compatibilidad y alineación de los objetivos del sistema de gestión con la política del sistema de gestión y los objetivos generales de la organización.

5.3 Establecer el programa de auditoría

5.3.1 Roles y responsabilidades de la persona que gestiona el programa de auditoría

La persona que gestiona el programa de auditoría debería:

— establecer el alcance del programa de auditoría;
— identificar y evaluar los riesgos del programa de auditoría;
— establecer responsabilidades de auditoría;
— establecer procedimientos para programas de auditoría;
— determinar los recursos necesarios;
— asegurar la implementación del programa de auditoría, incluyendo el establecimiento de objetivos, alcance y criterios de auditoría de las auditorías individuales, determinando los métodos de auditoría y seleccionando el equipo auditor y evaluando los auditores;
— asegurar el manejo y mantenimiento adecuado de los registros del programa de auditoría;
— monitorear, revisar y mejorar el programa de auditoría.

La persona que gestiona un programa de auditoría debería informar a la alta gerencia acerca del contenido del mismo y de ser necesario, debería solicitar su aprobación.

5.3.2 Competencia de la persona que gestiona el programa de auditoría

La persona que gestiona el programa de auditoría debería tener la competencia necesaria para gestionar dicho programa y los riesgos asociados de manera efectiva y eficiente, así como el conocimiento 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 de otra índole aplicables, relevantes a las actividades y productos del auditado;
— clientes, proveedores y otras partes interesadas del auditado, cuando sea aplicable.

La persona que gestiona el programa de auditoría debería involucrarse en actividades continuas de desarrollo profesional para mantener el conocimiento y habilidades necesarias para gestionar el programa de auditoría.

5.3.3 Establecer el alcance del programa de auditoría

La persona que gestiona el programa de auditoría debería determinar el alcance de dicho programa, el cual puede variar dependiendo el tamaño y naturaleza del auditado, así como de la naturaleza, funcionalidad, complejidad y nivel de madurez y temas significativos para el sistema de gestión a ser auditado.

NOTA En ciertos casos, dependiendo de la estructura o actividades del auditado, el programa de auditoría podría consistir solamente en una única auditoría (ej. una actividad pequeña de un proyecto).

Otros factores que impactan el alcance de 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 la auditoría de seguimiento, si aplica;
— el número, importancia, complejidad, similitud y ubicaciones de las actividades a ser auditadas;
— aquellos factores que influencian la efectividad del sistema de gestión;
— criterios aplicables de auditoría, tales como arreglos planeados para los requisitos de las normas de gestión, requisitos legales y contractuales y otros requisitos a los que la organización está suscrita;
— conclusiones de auditorías internas y externas previas;
— resultados de una revisión previa del programa de auditoría;
— temas de idioma, culturales y sociales;
— las inquietudes de las partes interesadas, tales como quejas de clientes o incumplimiento de requisitos legales;
— cambios significativos al auditado o sus operaciones;
— disponibilidad de la información y tecnologías de comunicación para soportar las actividades de auditoría; en particular, el uso de métodos de auditoría remotos (ver cláusula B.1);
— la ocurrencia de eventos internos y externos, tales como falla de productos, fugas de seguridad en la información, incidentes de salud y seguridad, actos criminales o incidentes ambientales.

5.3.4 Identificación y evaluación de los riesgos del programa de auditoría

Existen muchos riesgos diferentes asociados con el establecimiento, implementación, monitoreo, revisión y mejora de un programa de auditoría, que pueden afectar el logro de sus objetivos. La persona que gestiona el programa debería considerar estos riesgos para su desarrollo. Estos riesgos pueden estar asociados con lo siguiente:

— planeación; ej. Falla para establecer objetivos de auditoría relevantes y para determinar el alcance del programa de auditoría;
— recursos, ej. no permitir tiempo suficiente para desarrollar el programa de auditoría o para llevarlas a cabo;
— selección del equipo auditor, ej. el equipo no tiene la competencia colectiva para llevar a cabo auditorías de manera efectiva;
— implementación, ej. comunicación inefectiva del programa de auditoría;
— registros y su control, ej. falla para proteger adecuadamente los registros de auditoría que demuestren la efectividad del programa de auditoría;
— monitoreo, revisión y mejora del programa de auditoría, ej. monitoreo inefectivo de los resultados del programa de auditoría.

5.3.5 Establecer procedimientos para el programa de auditoría

La persona que gestiona el programa de auditoría debería establecer uno o más procedimientos que den tratamiento a lo siguiente, según sea aplicable:

— planeación y programación de auditorías teniendo en cuenta los riesgos del programa de auditoría;
— asegurar la seguridad y confidencialidad de la información;
— asegurar la competencia de los auditores y los líderes del equipo auditor;
— seleccionar equipos de auditoría apropiados y asignar sus roles y responsabilidades;
— llevar a cabo auditorías, incluyendo el uso de métodos de muestreo adecuados;
— conducir auditoría de seguimiento, si es necesario;
— reportar a la alta gerencia acerca del resultado general del programa de auditoría;
— mantener registros del programa de auditoría;
— monitorear y revisar el desempeño y riesgos y mejorar la efectividad del programa de auditoría.

5.3.6 Identificar los recursos del programa de auditoría

Al identificar los recursos necesarios para el programa de auditoría, la persona que gestiona dicho programa debería considerar:

— los recursos financieros necesarios para desarrollar, implementar, gestionar y mejorar las actividades de auditoría;
— métodos de auditoría;
— la disponibilidad de los auditores y expertos técnicos que tengan la competencia adecuada para los objetivos particulares del programa de auditoría;
— el alcance del programa de auditoría y los riesgos del mismo;
— tiempo y costos de viaje, hospedaje y otras necesidades de auditoría;
— la disponibilidad de la información y tecnologías de comunicación.

5.4 Implementación del programa de auditoría

5.4.1 Generalidades

La persona que gestiona el programa de auditoría debería implementar el programa de auditoría a través de lo siguiente:

— comunicar las partes pertinentes del programa de auditoría a las partes relevantes e informales periódicamente acerca del progreso;
— definir objetivos, alcance y criterios para cada auditoría individual;
— coordinar y programar auditorías y otras actividades relevantes al programa de auditoría;
— asegurar la selección de equipos de auditoría con la competencia necesaria;
— proveer los recursos necesarios a los equipos auditores;
— asegurar que las auditorías se lleven a cabo en concordancia con el programa de auditoría y dentro del marco de tiempo establecido;

— asegurar que las actividades de auditoría sean registradas y que los registros sean adecuadamente manejados y mantenidos.

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

Cada auditoría individual debería estar basada en objetivos, alcance y criterios de auditoría documentados. Estos deberían ser definidos por la persona que gestiona el programa de auditoría y deberían ser consistentes con los objetivos generales del programa de auditoría.

Los objetivos de auditoría definen lo que se debe lograr en la auditoría individual y pueden incluir lo siguiente:

— determinación del grado de conformidad del sistema de gestión a ser auditado, o pates de este, con los criterios de auditoría;
— determinación del grado de conformidad de las actividades, procesos y productos con los requisitos y procedimientos del sistema de gestión;
— evaluación de la capacidad del sistema de gestión para asegurar cumplimiento con los requisitos legales y contractuales y otros requisitos a los que la organización se suscriba;
— evaluación de la efectividad del sistema de gestión para cumplir sus objetivos especificados;
— identificación de áreas potenciales de mejora del sistema de gestión.

El alcance de la auditoría debería ser consistente con los objetivos y el programa de auditoría. Esto incluye factores como ubicaciones físicas, unidades organizacionales, actividades y procesos a ser auditados, así como el periodo de tiempo cubierto por la auditoría.

Los criterios de auditoría son usados como puntos de referencia para determinar la conformidad y pueden incluir políticas, procedimientos, normas, requisitos legales, requisitos del sistema de gestión, requisitos contractuales, códigos de conducta de sector y otros arreglos planeados aplicables.

En el evento de cambios a los objetivos, alcance o criterios de auditoría, el programa de auditoría debería ser modificado si es necesario.

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

5.4.3 Selección de métodos de auditoría

La persona que gestiona el programa de auditoría debería seleccionar y determinar los métodos para llevar a cabo una auditoría de manera efectiva, dependiendo de los objetivos, alcance y criterios de auditoría definidos.

NOTA El Anexo B proporciona una Guía sobre cómo determinar los métodos de auditoría.

Cuando dos o más organizaciones llevan a cabo una auditoría conjunta al mismo auditado, las personas que gestionan los diferentes programas de auditoría deberían ponerse de acuerdo sobre el método de auditoría y considerar las implicaciones para obtener los recursos y planear la auditoría. Si un auditado opera dos o más sistemas de gestión de diferentes disciplinas, las auditorías combinadas pueden ser incluidas en el programa de auditoría.

5.4.4 Selección de los miembros del equipo auditor

La persona que gestiona el programa de auditoría debería nombrar los miembros del equipo auditor, incluyendo el líder del equipo y cualquier experto técnico necesario para la auditoría específica.

Un equipo auditor debería ser seleccionado teniendo en cuenta la competencia necesaria para alcanzar los objetivos de la auditoría individual dentro del alcance definido. Si solo hay un auditor, éste auditor debería llevar a cabo todos los deberes aplicables a un líder de equipo.

NOTA El Capítulo 7 contiene una guía para determinar las competencias requeridas por los miembros del equipo auditor y describe el proceso de evaluación de auditores.

Al decidir sobre el tamaño y composición del equipo auditor para la auditoría específica, se debería prestar atención a lo siguiente:

a) la competencia general del equipo auditor requerida para alcanzar los objetivos de la auditoría, teniendo en cuenta el alcance y criterios de la misma;
b) la complejidad de la auditoría y si la auditoría es una auditoría combinada o conjunta;
c) los métodos de auditoría que han sido seleccionados;
d) requisitos legales y contractuales y otros requisitos a los que la organización esté suscrita;
e) la necesidad de asegurar la independencia de los miembros del equipo auditor de las actividades a ser auditadas y de evitar conflicto de intereses [ver principio e) en el Capítulo 4];
f) la habilidad de los miembros del equipo auditor para interactuar efectivamente con los representantes del auditado y de trabajar juntos;
g) el idioma de la auditoría, y las características sociales y culturales del auditado. Estos temas pueden ser cubiertos ya sea por las habilidades propias del auditor o a través del soporte de un experto técnico.

A fin de asegurar la competencia general del equipo auditor, se deberían tomar las siguientes mediadas:

— identificar el conocimiento y habilidades necesarias para alcanzar los objetivos de la auditoría;

— seleccionar los miembros del equipo auditor de manera tal que todo el conocimiento y habilidades necesarias estén presentes en el equipo.

Si los auditores que hacen parte del equipo auditor no cubren toda la competencia necesaria, se deberían incluir expertos técnicos con competencias adicionales en el equipo. Los expertos técnicos deberían operar bajo la dirección de un auditor pero no deberían actuar como auditores.

Se pueden incluir auditores en entrenamiento dentro del equipo auditor, pero estos deberían participar bajo la dirección y guía de un auditor.

Se pueden requerir ajustes al tamaño y composición del equipo auditor durante la auditoría, en caso de presentarse un conflicto de intereses o un tema de competencia. Si tales situaciones se presentan, estas deberían ser discutidas con las partes apropiadas (ej. líder del equipo auditor, la persona que gestiona el programa de auditoría, el cliente de auditoría o el auditado) antes de realizar cualquier ajuste.

5.4.5 Asignación de responsabilidad de una auditoría individual al líder del equipo auditor

La persona que gestiona el programa de auditoría debería asignar la responsabilidad de la realización de la auditoría individual al líder del equipo auditor.

La asignación debería hacerse con suficiente tiempo antes de la fecha de la auditoría, a fin de asegurar una planeación efectiva de la misma.

Para asegurar la conducción efectiva de auditorías individuales, se debería entregar la siguiente información al líder del equipo auditor:

a) objetivos de auditoría;
b) criterios de auditoría y cualquier documento de referencia;
c) alcance de auditoría, incluyendo la identificación de las unidades organizacionales y funcionales y los procesos a ser auditados;
d) métodos y procedimientos de auditoría;
e) composición del equipo auditor;
f) detalles de contacto del auditado, las locaciones, fechas y duración de las actividades de auditoría que se van a llevar a cabo;
g) adjudicación de recursos apropiados para llevar a cabo la auditoría;
h) información necesaria para evaluar y tratar los riesgos identificados para el alcance de los objetivos de auditoría.

La información de asignación también debería cubrir lo siguiente, según sea apropiado:
— idioma de trabajo y de reporte de la auditoría cuando éste es diferente del idioma del auditor o del auditado, o de ambos;
— contenido y distribución del reporte de auditoría requerido por el programa de auditoría;

— temas relacionados con confidencialidad y seguridad de la información, si lo requiere el programa de auditoría;
— cualquier requisitos de salud y seguridad para los auditores;
— cualquier requisitos de seguridad y autorizaciones;
— cualquier acción de seguimiento, ej., de una auditoría previa, si aplica;
— coordinación con otras actividades de auditoria, en el caso de una auditoría conjunta.

Cuando se lleva a cabo una auditoría conjunta, es importante llegar a un acuerdo entre las organizaciones que conducen la auditoría, antes del inicio de la misma, sobre las responsabilidades específicas de cada parte, en particular en lo relacionado a la autoridad del líder del equipo auditor nombrado para la auditoría.

5.4.6 Gestión del resultado del programa de auditoría

La persona que gestiona el programa de auditoría debería asegurar que se lleven a cabo las siguientes actividades:
— revisar y aprobar los reportes de auditoría, incluyendo la evaluación de idoneidad y conveniencia de los hallazgos de auditoría;
— revisar el análisis de causa raíz y la efectividad de las acciones correctivas o preventivas;
— distribución de los reportes de auditoría a la alta gerencia y otras partes relevantes;
— determinar la necesidad de una auditoría de seguimiento.

5.4.7 Gestión y mantenimiento de registros de programa de auditoría

La persona que gestiona el programa de auditoría debería asegurar que se creen, gestionen y mantengan los registros de auditoría para demostrar la implementación de un programa de auditoría. Se deberían establecer procesos para asegurar que cualquier necesidad de confidencialidad asociada con los registros de auditoría sea cubierta.

Los registros deberían incluir los siguientes:

a) registros relacionados con el programa de auditoría, tales como:
— objetivos y alcance del programa de auditoría documentados;
— aquellos que tratan los riesgos del programa de auditoría;
— revisiones de la efectividad del programa de auditoría;

b) registros relacionados con cada auditoría individual, tales como:
— planes y reportes de auditoría;
— reportes de no conformidad;
— reportes de acciones correctivas y preventivas;
— reportes de auditoría de seguimiento, si aplica;

c) registros relacionados con personal de auditoria que cubren temas como:
— competencia y evaluación de desempeño de los miembros del equipo auditor;
— selección de equipos de auditoría y miembros de equipo;
— mantenimiento y mejora de la competencia.

La forma y nivel de detalle de los registros debería demostrar que los objetivos del programa de auditoría han sido alcanzados.

5.5 Monitoreo del programa de auditoría

La persona que gestiona el programa de auditoría debería monitorear su implementación, teniendo en cuenta la necesidad de:

a) evaluar conformidad con los programas de auditoría, cronogramas y objetivos de auditoría;
b) evaluar el desempeño de los miembros del equipo auditor;
c) evaluar la habilidad de los equipos auditores para implementar el plan de auditoría;
d) evaluar la retroalimentación dada por parte de la alta gerencia, auditados, auditores y otras partes interesadas.

Algunos factores pueden determinar la necesidad de modificar el programa de auditoría; estos pueden incluir:

— hallazgos de auditoría;
— nivel demostrado de efectividad del sistema de gestión;
— cambios en el sistema de gestión del cliente o del auditado;
— cambios en las normas, requisitos legales y contractuales y otros requisitos a los que la organización se suscriba;
— cambio de proveedor.

5.6 Revisión y mejora del programa de auditoría

La persona que gestiona el programa de auditoría debería revisar dicho programa para evaluar si se han alcanzado sus objetivos. Las lecciones aprendidas del programa de auditoría deberían ser usadas como elementos de entrada para el proceso de mejora continua del programa.

La revisión del programa de auditoría debería considerar lo siguiente:

a) resultados y tendencias del monitoreo del programa de auditoría;
b) conformidad con los procedimientos del programa de auditoría;
c) necesidades y expectativas cambiantes de las partes interesadas;
d) registros del programa de auditoría;
e) métodos nuevos o alternativos de auditoría;
f) efectividad de las mediadas tomadas para tratar los riesgos asociados con el programa de auditoría;
g) temas de confidencialidad y seguridad de la información relacionados con el programa de auditoría.

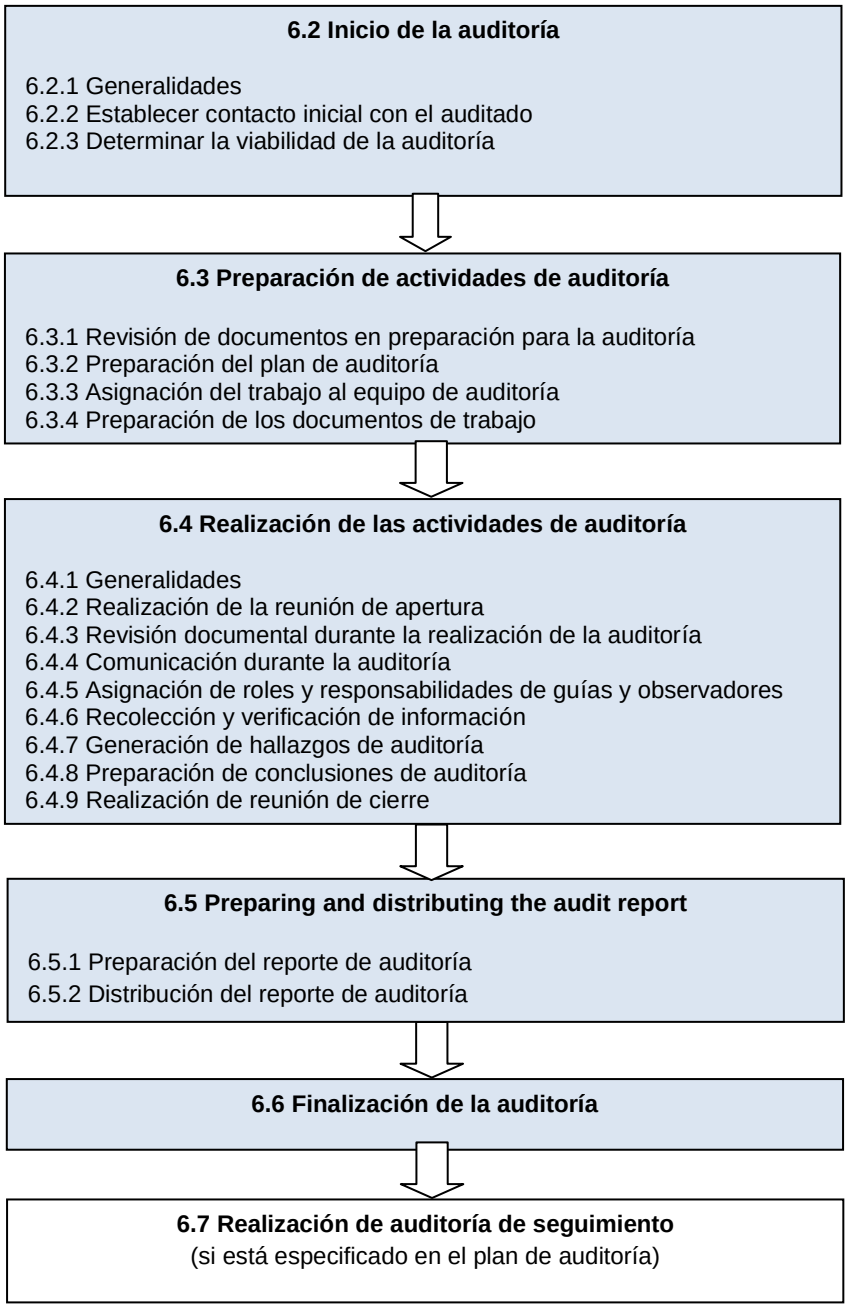
La persona que gestiona el programa de auditoría debería revisar la implementación general del programa, identificar áreas de mejora, enmendar el programa si es necesario, y también debería:

— revisar el continuo desarrollo profesional de los auditores, en concordancia con 7.4, 7.5 y 7.6;
— reportar los resultados de la revisión del programa de auditoría a la alta gerencia.

6 Realización de la auditoría

6.1 Generalidades

Este capítulo proporciona orientación sobre la planificación y forma de llevar a cabo 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 del objetivo y alcance de cada auditoría específica.



NOTE La numeración de sub-cláusulas hace referencia a las sub-cláusulas relevantes en esta Norma Internacional.

Figura 2 — Actividades típicas de auditoría

6.2 Inicio de la auditoría

6.2.1 Generalidades

Cuando se da inicio a una auditoría, la responsabilidad de llevar a cabo dicha auditoría sigue siendo del líder del equipo auditor (ver 5.4.5) hasta que la auditoría se haya finalizado (ver 6.6).

Para iniciar una auditoría, se deberían tener en cuenta los pasos de la Figura 2; sin embargo, la secuencia puede diferir dependiendo de el auditado, los procesos y otras circunstancias específicas de la auditoría.

6.2.2 Establecer contacto inicial con el auditado

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

— establecer comunicación con los representantes del auditado;
— confirmar la autoridad para la realización de la auditoría;
— proveer información sobre los objetivos, alcance y métodos de auditoría, así como la composición del equipo auditor, incluyendo los expertos técnicos;
— solicitar acceso a documentos y registros relevantes para propósitos de planeación;
— determinar requisitos legales y contractuales aplicable y otros requisitos relevantes a las actividades y productos del auditado;
— confirmar el acuerdo del auditado en lo referente al grado de divulgación y tratamiento de la información confidencial;
— hacer arreglos para la auditoría, incluyendo la programación de fechas;
— determinar cualquier requisito específico de la locación en cuanto a acceso, seguridad, salud y seguridad y otros;
— llegar a acuerdos sobre la participación de observadores y la necesidad de guías para el equipo auditor;
— determinar cualquier área de interés o inquietud del auditado en relación a la auditoría específica.

6.2.3 Determinación de la viabilidad de la auditoría

La viabilidad de la auditoría debería ser determinada a fin de proveer una confianza razonable de que los objetivos de auditoría pueden ser alcanzados.

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

— información suficiente y apropiada para la planeación y realización de la auditoría;
— cooperación adecuada por parte del auditado;
— tiempo y recursos adecuados para la realización de la auditoría.

Cuando la auditoría no resulta viable, se debería proponer una alternativa al cliente de auditoría en acuerdo con el auditado.

6.3 Preparación de actividades de auditoría

6.3.1 Revisión de documentos en preparación para la auditoría

La documentación relevante del sistema de gestión del auditado debería ser revisada con el fin de:

— reunir información para preparar actividades de auditoria y documentos de trabajo aplicables (ver 6.3.4), ej. sobre los procesos, funciones;
— establecer una visión general del grado de documentación del sistema de gestión para detectar posibles vacíos.

NOTA El Capítulo B2 provee una guía sobre cómo llevar a cabo la revisión documental.

Lo documentación debería incluir, según sea aplicable, los documentos y registros del sistema de gestión, así como reportes de auditorías previas. La revisión documental debería tener en cuenta el tamaño, naturaleza y complejidad del sistema de gestión y organización del auditado, así como los objetivos y 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 entregada por el auditado. El plan de auditoría debería considerar el efecto de las actividades de auditoría en los procesos del auditado y proveer la base para el acuerdo entre el cliente de auditoría, el equipo auditor y el auditado referente a la realización de la auditoría. El plan debería facilitar la programación y coordinación eficiente de las actividades de auditoría a fin de alcanzar efectivamente los objetivos.

La cantidad de detalle entregada en el plan de auditoría debería reflejar el alcance y complejidad de la auditoría, así como el efecto de incertidumbre sobre el logro de los objetivos de auditoría. Al preparar el plan de auditoría, el líder del equipo auditor debería considerar lo siguiente:

— las técnicas de muestreo apropiadas (ver Capítulo B.3);
— la composición del equipo auditor y su competencia colectiva;
— el riesgo creado por la auditoría para la organización.

Por ejemplo, los riesgos a la organización pueden dar como resultado que la presencia del equipo auditor influencie la salud y seguridad, ambiente y calidad, y su presencia puede generar amenazas a los productos, servicios, personal o infraestructura del auditado (ej. contaminación en instalaciones de cuartos limpios).

Para auditorías combinadas, se debería prestar atención particular a las interacciones entre los procesos operativos y los objetivos y prioridades de los diferentes sistemas de gestión.

6.3.2.2 La escala y contenido el plan de auditoría puede diferir, por ejemplo, entre la auditoría inicial y auditorías subsecuentes, así como entre auditorías internas y externas. El plan de auditoría debería ser lo suficientemente flexible para permitir cambios que se puedan hacer necesarios durante el progreso de las actividades de auditoría.

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

a) los objetivos de la auditoría;
b) el alcance de auditoría, incluyendo la identificación de las unidades organizacionales y funcionales, así como los procesos a ser auditados;
c) los criterios de auditoría y cualquier documento de referencia;
d) la ubicación, fechas, tiempo esperado y duración de las actividades de auditoría a realizar, incluyendo reuniones con la gerencia del auditado;
e) los métodos de auditoría a utilizar, incluyendo el grado de muestreo requerido para obtener suficiente evidencia de auditoría y el diseño del plan de muestreo, si aplica;
f) los roles y responsabilidades de los miembros del equipo auditor, así como de los guías y observadores;
g) la adjudicación de recursos apropiados para áreas críticas de la auditoría.

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

— identificación de los representantes del auditado para la auditoría;
— el idioma de trabajo y de reporte de la auditoría, cuando este sea diferente del idioma del auditor o auditado o ambos;
— los temas del reporte de auditoría;
— arreglos de logística y de comunicaciones, incluyendo arreglos específicos par alas ubicaciones a ser auditadas;
— cualquier medida específica a tomar para tratar el efecto de incertidumbre de alcanzar los objetivos de auditoría;
— temas relacionados con confidencialidad y seguridad de la información;
— cualquier acción de seguimiento de una auditoría previa;
— cualquier actividad de seguimiento a la auditoría planeada;
— coordinación con otras actividades de auditoría, en caso de una auditoría conjunta.

El plan de auditoría puede ser revisado y aceptado por el cliente de auditoría y debería ser presentado al auditado. Cualquier objeción por parte del auditado al plan de auditoría debería ser resuelta entre el líder del equipo auditor y el cliente de auditoría.

6.3.3 Asignación de trabajo 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, funciones, lugares, áreas o actividades específicos. Tales asignaciones deberían tener en cuenta la necesidad de independencia y competencia de los auditores, y el uso eficaz de los recursos, así como las diferentes funciones y responsabilidades de los auditores, auditores en formación y

expertos técnicos. Se pueden realizar cambios en la asignación de tareas a medida que la auditoría se va llevando a cabo para asegurarse de que se cumplen los objetivos de la auditoría.

6.3.4 Preparación de los documentos de trabajo

Los miembros del equipo auditor deberían recolectar y revisar la información pertinente a las tareas asignadas y preparar los documentos de trabajo que sean necesarios como referencia y registro del desarrollo de la auditoría. Tales documentos de trabajo pueden incluir:

— listas de verificación;
— planes de muestreo de auditorías;
— formularios para registrar información, tal como evidencias de apoyo, hallazgos de 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 La Cláusula B.4. provee guía sobre la preparación de documentos de trabajo.

Los documentos de trabajo, incluyendo los registros que resultan de su uso, deberían retenerse al menos hasta que finalice la auditoría, o de acuerdo con lo especificado 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 de propiedad privada deberían ser guardados con la seguridad apropiada en todo momento por los miembros del equipo auditor.

6.4 Realización de actividades de auditoría

6.4.1 Generalidades

Las actividades de auditoría normalmente son llevadas a cabo en una secuencia definida, tal como se indica en la Figura 2. Esta secuencia puede ser modificada para ajustarse 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 que todas las partes están de acuerdo con el plan de auditoría (auditado, equipo auditor);
b) presentar al equipo auditor;
c) asegurar que se pueden llevar a cabo todas las actividades de auditoría planeadas.

Se debería realizar una reunión de apertura con la dirección del auditado o, cuando sea apropiado, con aquellos responsables para las funciones o procesos que se van a auditar. Durante la reunión de apertura se debería dar la oportunidad de hacer preguntas.

El grado de detalle debería ser consistente con la familiaridad del auditado con los procesos. En muchos caso, ej. auditorías internas en organizaciones pequeñas, la reunión de apertura puede consistir simplemente en comunicar que se está realizando una auditoría y explicar la naturaleza de la misma.

Para otras situaciones de auditoría la reunión puede ser formal o se deberían guardar registros de asistencia. La reunión debería ser presidida por el líder del equipo auditor y se deberían tener en cuenta los siguientes elementos, según resulte apropiado:

— presentación de los participantes, incluyendo observadores y guías y una generalidad de sus roles;
— confirmación de los objetivos, alcance y criterios de auditoría;
— confirmación del plan de auditoría y otras disposiciones pertinentes con el auditado, tales como la fecha y hora de la reunión de cierre, cualquier reunión intermedia del equipo auditor y la gerencia del auditado y cambios tardíos;
— presentación de los métodos a utilizar durante la auditoría, incluyendo el informar al auditado que la evidencia estará basada en una muestra de la información disponible;
— presentación de los métodos para gestionar los riesgos que pueda implicar para la organización la presencia de los miembros del equipo auditor;
— confirmación de canales formales de comunicación entre el equipo auditor y el auditado;
— confirmación del idioma a usar durante la auditoría;
— confirmación de que durante la auditoría, el auditado será constantemente informado del progreso de la auditoría;
— confirmación de que los recursos e instalaciones requeridos por el equipo auditor están disponibles;
— confirmación de temas relacionados con confidencialidad y seguridad de la información;
— confirmación de procedimientos relevantes de salud y seguridad y emergencia para el equipo auditor;
— información sobre el método de reporte de los hallazgos de auditoría, incluyendo su calificación, de haberla;
— información acerca de las condiciones bajo las cuales se dará por finalizada la auditoría;
— información acerca de la reunión de cierre;
— información acerca de cómo dar tratamiento a posibles hallazgos durante la auditoría;
— información acerca de cualquier sistema usado para recibir retroalimentación por parte del auditado sobre los hallazgos o conclusiones de la auditoría, incluyendo quejas y apelaciones.

6.4.3 Revisión documental durante la realización de la auditoría

La documentación relevante del auditado debería ser revisada para:

— determinar la conformidad del sistema, en cuanto a su documentación, con los criterios de auditoría;
— recopilar información para soportar las actividades de auditoria.

NOTA El Capítulo B2 proporciona una Guía sobre como llevar a cabo la revisión documental.

La revisión puede estar combinada con otras actividades de auditoría y puede continuar a todo lo largo de la misma, en tanto esto no vaya en detrimento de la efectividad en la realización de la auditoría.

Si no se puede proveer documentación adecuada durante el marco de tiempo dado en el plan de auditoría, el líder del equipo auditor debería informar este hecho tanto a la persona que gestiona el programa de auditoría como al auditado. Dependiendo de los objetivos y alcance de la auditoría, se debería tomar una decisión respecto a si esta se debe continuar o suspender hasta una vez se solucionen las dificultades con la documentación.

6.4.4 Comunicación durante la auditoría

Durante la auditoría puede resultar necesario hacer arreglos formales de comunicación entre el equipo auditor, así como con el auditado, el cliente de auditoría y potenciales entes externos (ej. entes reguladores), especialmente cuando los requisitos legales incluyen el reporte obligatorio de no conformidades.

El equipo de auditoría debería reunirse periódicamente para intercambiar información, evaluar el progreso de la auditoría y re-asignar trabajo entre los miembros del equipo auditor, según resulte necesario.

Durante la auditoría, el líder del equipo auditor debería comunicar periódicamente el progreso de la auditoría y cualquier duda al auditado y cliente de auditoría, según sea apropiado. La evidencia recolectada durante la auditoría que sugiera un riesgo significativo inminente para el auditado debería ser reportado sin demora al auditado, y cuando sea apropiado, al cliente de auditoría. Cualquier inquietud acerca de temas que están por fuera del alcance de la auditoría debería ser notada y reportada al líder del equipo auditor, para su posible comunicación al cliente de auditoría y al auditado.

Cuando la evidencia de auditoría disponible indique que no se pueden alcanzar los objetivos de auditoría, el líder del equipo auditor debería reportar las razones al cliente de auditoría y al auditado para determinar las acciones apropiadas. Tales acciones pueden incluir la re-confirmación o modificación del plan de auditoría, cambios a los objetivos o alcance de la auditoría, o finalización de la misma.

Cualquier necesidad de realizar cambios al plan de auditoría que se puedan hacer aparentes durante el progreso de las actividades de auditoría debería ser revisada y aprobados, si es apropiado, tanto por la persona que gestiona el programa de auditoría como por el auditado.

6.4.5 Asignación de roles y responsabilidades de guías y observadores

Los guías y observadores (ej. entes reguladores u otras partes interesadas) pueden acompañar al equipo de auditores. Estos no deberían influenciar o interferir con la realización de la auditoría. Si esto no se puede asegurar, el líder del equipo auditor debería tener el derecho de negar a los observadores la participación en ciertas actividades de auditoría.

Para los observadores, cualquier obligación relacionada con salud y seguridad y confidencialidad y seguridad de la información debería ser manejada entre el cliente de auditoría y el auditado.

Los guías nombrados por el auditado, deberían ayudar al equipo auditor y actuar a petición del líder del equipo auditor.

Sus responsabilidades deberían incluir las siguientes:

a) ayudar a los auditores a identificar a los individuos que van a participar en las entrevistas y confirmar los tiempos;
b) organizar la logística de acceso a locaciones específicas del auditado;
c) asegurar que el equipo auditor y los observadores conocen y respetan las reglas relacionadas con la seguridad de la ubicación y los procedimientos de emergencia.

El rol del guía también puede incluir lo siguiente:

— ser testigo de la auditoría en nombre del auditado;
— proveer aclaraciones o ayudar a recolectar información.

6.4.6 Recolección y Verificación de la información

Durante la auditoría, la información relevante a los objetivos, alcance y criterios de la auditoría, incluyendo información relacionada con interfaces entre funciones, actividades y procesos debería ser recolectada por medio de muestreo apropiado y debería ser verificada. Solo información verificable debería ser aceptada como evidencia de auditoría. La evidencia de auditoría que conduce a hallazgos de auditoría debería ser registrada. Si durante la recolección de evidencia el equipo auditor conoce de circunstancias o riesgos nuevos o cambiantes, estos deberían ser tratados por el equipo de manera concordante.

NOTA 1 El Capítulo B3 provee una Guía sobre muestreo

La Figura 3 provee una visión general del proceso, dese la recolección de información hasta llegar a conclusiones de auditoría.

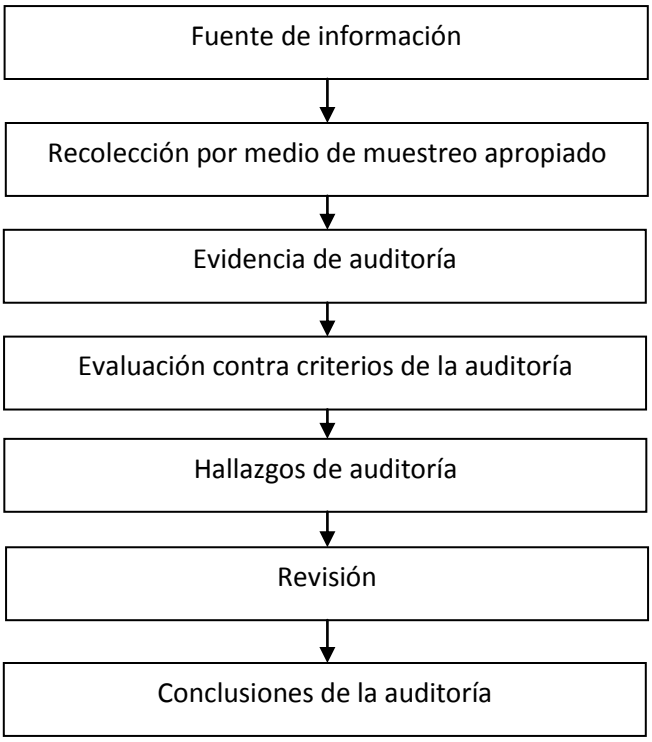


Figura 3 — Visión general del proceso de recolectar y verificar información

Los métodos para recolectar información incluyen los siguientes:

— entrevistas;
— observaciones;
— revisión de documentos, incluidos registros.

NOTA 2 El Capítulo B.5. provee una Guía sobre fuentes de información.

NOTA 3 El Capítulo B.6. Provee lineamientos sobre la visita a las instalaciones del auditado.

NOTA 4 El Capítulo B.7. Provee una Guía sobre cómo llevar a cabo entrevistas.

6.4.7 Generación de hallazgos de auditoría

La evidencia de auditoría debería ser evaluada contra los criterios de la auditoría a fin de determinar los hallazgos de la auditoría. Los hallazgos de auditoría pueden indicar conformidad o no conformidad con los criterios de la auditoría. Cuando el plan de auditoría así lo especifique, los hallazgos individuales de auditoría deberían incluir conformidad y buenas prácticas junto con su evidencia de soporte, oportunidades de mejora y recomendaciones para el auditado.

Las no conformidades y su soporte de evidencia de auditoría deberían ser registradas. Las no conformidades pueden estar clasificadas. Estas deberían ser revisadas con el auditado a fin de obtener reconocimiento de que la evidencia de auditoría es correcta y que las no conformidades son entendidas. Se debería realizar todo intento de resolver opiniones divergentes relacionadas con la evidencia o hallazgos de auditoría; cualquier punto sin resolver debería ser registrado.

El equipo de auditoría debería reunirse con la frecuencia que sea necesaria para revisar los hallazgos de auditoría a intervalos adecuados durante la auditoría.

NOTA El Capítulo B.8. presenta una guía adicional sobre la identificación y evaluación de hallazgos de auditoría.

6.4.8 Preparación de conclusiones de auditoría

El equipo auditor debería reunirse antes de la reunión de cierre con el fin de:

a) revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma;
b) llegar a un acuerdo respecto a las conclusiones, teniendo en cuenta la incertidumbre inherente en el proceso de auditoría;
c) preparar recomendaciones, si esto está especificado en el plan de auditoría;
d) discutir el seguimiento a la auditoría, según sea aplicable.

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

— el grado de conformidad con los criterios de la auditoría y la robustez del sistema de gestión, incluyendo la efectividad del sistema de gestión para cumplir con los objetivos establecidos;
— la efectiva implementación, mantenimiento y mejora del sistema de gestión;
— la capacidad del proceso de revisión por la dirección de asegurar la continua idoneidad, capacidad, efectividad y mejora del sistema de gestión;
— logro de los objetivos de auditoria, cubrimiento del alcance de la auditoría y cumplimiento con los criterios de la auditoría;
— causas raíz de los hallazgos, si está especificado en el plan de auditoría;
— hallazgos similares encontrados en diferentes áreas auditadas con el propósito de identificar tendencias.

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

6.4.9 Realización de la reunión de cierre

Se debería llevar a cabo una reunión de cierre, facilitada por el líder del equipo auditor, para presentar los hallazgos y conclusiones de la auditoría. Los participantes de la reunión de cierre deberían incluir la gerencia del auditado y, cuando sea apropiado, aquellos responsables por las funciones o procesos que han sido auditados, y también

pueden incluir al cliente de auditoría u otras partes. Si es necesario, el líder del equipo auditor debería prevenir al auditado de las situaciones encontradas durante la auditoría que pudieran disminuir la confianza en las conclusiones de la auditoría.

Si está definido en el sistema de gestión, o por acuerdo con el cliente de auditoría, los participantes deberían llegar a un acuerdo sobre el intervalo de tiempo para que el auditado presente un plan de acción para dar tratamiento a los hallazgos de auditoría.

El grado de detalle debería ser consistente 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 otros casos, como en el caso de auditorías internas, la reunión de cierre es menos formal y puede consistir solo en comunicar los hallazgos y conclusiones de la auditoría.

Según sea apropiado, se debe explicar lo siguiente al auditado durante la reunión de cierre:

— prevenir respecto a que la evidencia de auditoría recolectada está basada en una muestra de la información disponible;
— el método de reporte;
— el proceso de manejo de hallazgos de auditoría y las posibles consecuencias;
— presentación de los hallazgos y conclusiones de auditoría de manera tal que sean comprendidas y reconocidas por la gerencia del auditado;
— cualquier actividad post-auditoría relacionada (ej. implementación de acciones correctivas, manejo de quejas de auditoría, proceso de apelación).

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

Si los objetivos de la auditoría así lo especifican, se pueden presentar recomendaciones de mejora. Se debería enfatizar que dichas recomendaciones no son obligatorias.

6.5 Preparación y distribución del reporte de auditoría

6.5.1 Preparación del reporte de auditoría

El líder del equipo auditor debería reportar los resultados de acuerdo con los procedimientos del programa de auditoria.

El reporte de auditoría debería proveer un registro complete, exacto, 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) identificación del cliente de auditoría;
d) identificación del equipo auditor y los participantes del auditado en la auditoría;

e) las fechas y los lugares donde se realizaron las actividades de auditoría;
f) los criterios de auditoría;
g) los hallazgos de la auditoría y la evidencia relacionada;
h) las conclusiones de la auditoría;
i) una declaración sobre el grado en el cual se han cumplido los criterios de la auditoría.

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

— el plan de auditoría incluyendo la programación de tiempos;
— un resumen del proceso de auditoría, incluyendo cualquier obstáculo encontrado que pueda disminuir la confianza en las conclusiones de la auditoría;
— confirmación de que se han alcanzado los objetivos de la auditoría dentro del alcance, de acuerdo con el plan de auditoría;
— áreas no cubiertas incluidas dentro del alcance de la auditoría;
— un resumen que cobra las conclusiones de la auditoría y los principales hallazgos de auditoría que las soportan;
— cualquier opinión divergente sin resolver entre el equipo auditor y el auditado;
— oportunidades de mejora, si está especificado en el plan de auditoría;
— buenas prácticas identificadas;
— planes de acción acordados, si los hubiese;
— una declaración de la naturaleza confidencial de los contenidos;
— cualquier implicación para el programa de auditoría o auditorías subsecuentes;
— la lista de distribución del reporte de auditoría.

NOTA El reporte de auditoría puede ser desarrollado antes de la reunión de cierre.

6.5.2 Distribución del reporte de auditoría

El reporte de auditoría debería ser emitido dentro de un periodo de tiempo acordado. En caso de demoras, las razones deberían ser comunicadas a la persona que gestiona el programa de auditoría.

El reporte de la auditoría debería estar fechado, revisado y aprobado, según aplique, de acuerdo con los procedimientos del programa de auditoría.

El reporte de la auditoría debería entonces der distribuido a los receptores designados en los procedimientos o plan de auditoría.

6.6 Finalización de la auditoría

La auditoría finalice cuando todas las actividades de auditoría planeadas hayan sido llevadas a cabo, o acordadas de otro modo con el cliente de auditoria (ej. puede presentarse una situación inesperada que no permita que la auditoría sea completada 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 sea requerido por ley, el equipo auditor y los responsables de la gestión del programa de auditoría no deberían revelar el contenido de los documentos, cualquier otra información obtenida durante la auditoría, ni el reporte de la 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 a raíz de la auditoría deberían ser incluidas en el proceso de mejora continua del sistema de gestión de las organizaciones auditadas.

6.7 Realización de seguimiento a la auditoría

Dependiendo de los objetivos de la auditoría, las conclusiones de la auditoría pueden indicar la necesidad de acciones correctivas, preventivas, o de mejora. Tales acciones generalmente son decididas y emprendidas por el auditado en un intervalo de tiempo acordado. Según sea apropiado, el auditado debería mantener informados a la persona que gestiona el programa de auditoría y al equipo auditor acerca del estatus de estas acciones.

La finalización y efectividad de estas acciones debería ser verificada. Esta verificación puede ser parte de una auditoría posterior.

7 Competencia y evaluación de auditores

7.1 Generalidades

La fiabilidad en el proceso de auditoría y la habilidad de alcanzar sus objetivos dependen de la competencia de aquellos individuos involucrados en la planeación y realización de auditorías, incluyendo auditores y líderes de equipo auditor.

La competencia debería ser evaluada a través de un proceso que tiene en cuanta el comportamiento personal y la habilidad de aplicar el conocimiento y habilidades ganadas a través de la educación, experiencia laboral, entrenamiento de auditor y experiencia en auditoría.

Este proceso debería tener en cuenta las necesidades y objetivos del programa de auditoría. Algunos de los conocimientos y habilidades descritas en 7.2.3 son comunes a los auditores de cualquier disciplina de sistema de gestión; otras son específicas a disciplinas individuales de sistemas de gestión. No es necesario que todos los auditores del equipo auditor tengan la misma competencia; sin embargo, la competencia general del equipo auditor debe ser suficiente para alcanzar los objetivos de la auditoría.

La evaluación de las competencias de un auditor debería ser planeada, implementada y documentada de acuerdo con el programa de auditoría, incluyendo sus procedimientos para entregar un resultado que sea objetivo, consistente, justo y confiable. El proceso de evaluación debería incluir cuatro pasos principales, así:

a) determinar la competencia del personal de auditoría para suplir las necesidades del programa de auditoría;
b) establecer los criterios de evaluación;
c) seleccionar el método de evaluación apropiado;
d) llevar a cabo la evaluación.

El resultado del proceso de evaluación debería proveer una base para lo siguiente:

— selección de miembros de equipo auditor según lo descrito en 5.4.4;
— determinación de la necesidad de competencia mejorada (ej. entrenamiento adicional);
— evaluación constante de desempeño de auditores.

Los auditores deberían desarrollar, mantener y mejorar sus competencias a través del desarrollo profesional continuo y la participación regular en auditorías (ver 7.6).

En 7.4 y 7.5 se describe un proceso para evaluar los auditores y líderes de equipo.

Los auditores y líderes de equipo auditor deberían ser evaluados contra los criterios presentados en 7.2.2 y 7.2.3.

La competencia requerida por la persona que gestiona el programa de auditoría se describe en 5.3.2.

7.2 Determinación de las competencias de auditor requeridas para satisfacer las necesidades del programa de auditoría

7.2.1 Generalidades

Al decidir el conocimiento y habilidades apropiadas requeridas por el auditor, se debe tener en cuenta lo siguiente:

— el tamaño, naturaleza y complejidad de la organización a ser auditada;
— las disciplinas de sistema de gestión a ser auditada;
— los objetivos y alcance del programa de auditoría;
— otros requisitos, tales como aquellos impuestos por entes externos, cuando sea apropiado;
— el rol del proceso de auditoría en el sistema de gestión del auditado;
— la complejidad del sistema de gestión a ser auditado;
— la incertidumbre para alcanzar los objetivos de la auditoría.

Esta información debería ser cruzada con la que se encuentra listada 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 auditoría descritos en el Capítulo 4. Los auditores deberían mostrar un comportamiento profesional durante el desarrollo 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, instintivamente consciente y capaz de entender las situaciones;
— versátil, es decir, se adapta fácilmente a diferentes situaciones;
— tenaz, es decir, persistente, orientado hacia el logro de los objetivos;
— decidido, es decir, alcanza conclusiones oportunas basadas en el análisis y razonamiento lógicos;
— seguro de sí mismo, es decir, actúa y funciona de forma independiente a la vez que se relaciona eficazmente con otros;
— actúa con Fortaleza, es decir, capaz de actuar ética y responsablemente aún cuando dichas acciones no siempre sean populares y a veces puedan resultar en desacuerdo o confrontación;
— abierto a la mejora, es decir, dispuesto a aprender de las situaciones, y en búsqueda de mejores resultados de auditoría;
— sensible culturalmente, es decir, observante y respetuosos de la cultura del auditado;
— colaborador, es decir, que interactúa eficientemente con otros, incluyendo los miembros del equipo auditor y el personal del auditado.

7.2.3 Conocimiento y habilidades

7.2.3.1 Generalidades

Los auditores deberían poseer el conocimiento y habilidades necesarias para alcanzar los resultados esperados de las auditorías que se espera que realicen. Todos los auditores deberían tener conocimientos y habilidades genéricas y se debería esperar también que posean algún conocimiento y habilidades específicos al sector o la disciplina. Los líderes de equipo auditor deberían además tener el conocimiento y habilidades necesarias para entregar liderazgo al equipo de auditoría.

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

Los auditores deberían tener el conocimiento y habilidades en las áreas descritas a continuación.

a) **Principios, procedimientos y métodos de auditoría**: los conocimientos y experiencia en esta área habilitan al auditor para aplicar los principios, procedimientos y métodos

apropiados a diferentes auditorías, y para asegurar que las auditorías sean realizadas de manera consistente y sistemática. Un auditor debería ser capaz de hacer lo siguiente:

— aplicar principios, procedimientos y técnicas de auditoría,
— planificar y organizar el trabajo eficazmente,
— llevar a cabo la auditoría dentro del horario acordado,
— establecer prioridades y centrarse en los asuntos de importancia,
— recopilar información a través de entrevistas eficaces, escuchando, observando y revisando documentos, registros y datos;
— entender y considerar las opiniones de los expertos;
— entender lo apropiado del uso de técnicas de muestreo y sus consecuencias para la auditoría,
— verificar la relevancia 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 aquellos factores que puedan afectar a la fiabilidad de los hallazgos y conclusiones de la auditoría,
— utilizar los documentos de trabajo para registrar las actividades de la auditoría;
— documentar los hallazgos de auditoría y prepara reportes de auditoría apropiados;
— mantener la confidencialidad y seguridad de la información, datos, documentos y registros;
— comunicar efectivamente, oralmente y por escrito (ya sea personalmente o a través del uso de intérpretes y traductores);
— entender los tipos de riesgo asociados a la auditoría.

b) **Documentos del sistema de gestión y de referencia**: el conocimiento y habilidades en esta área capacitan al auditor para comprender el alcance de la auditoría y aplicar los criterios de auditoría, y deberían cubrir lo siguiente:

— normas de sistemas de gestión u otros documentos usados como criterios de auditoría;
— la aplicación de las normas de sistemas de gestión por parte del auditado y otras organizaciones, según sea apropiado;
— interacción entre los componentes del sistema de gestión;
— reconocer la jerarquía de los documentos de referencia;
— aplicación de los documentos de referencia a diferentes situaciones de auditoría.

c) **Contexto organizacional**: el conocimiento y habilidades en esta área capacitan al auditor para comprender la estructura del auditado, así como su negocio y prácticas gerenciales y debería cubrir lo siguiente:

— tipos organizacionales, gobierno, tamaño, estructura, funciones y relaciones;
— conceptos generales de negocio y gerencia, procesos y terminología relacionada, incluyendo planeación, presupuesto y manejo de personal;
— aspectos sociales y culturales del auditado.

d) **Requisitos legales y contractuales aplicables y otros requisitos que apliquen al auditado**: los conocimientos y habilidades en esta área capacitan al auditor para ser consciente y trabajar dentro de los requisitos legales y contractuales de la organización. El

conocimiento y habilidades específicas a la jurisdicción o a las actividades y productos del auditado deberían cubrir lo siguiente:

— leyes y regulaciones y sus agencias gobernantes;
— terminología legal básica;
— contratación y responsabilidad.

7.2.3.3 Conocimiento y habilidades específicas de la disciplina o sector de los auditores de sistemas de gestión

Los auditores deberían tener el conocimiento y habilidades específicas para la disciplina y sector que sean apropiados para auditor un tipo particular de sistema de gestión y sector.

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

El conocimiento y habilidades específicos al sector y disciplina incluyen lo siguiente:

— requisitos y principios de sistemas de gestión específicos a la disciplina, y su aplicación;
— requisitos legales relevantes a la disciplina y el sector, de manera tal que el auditor conozca los requisitos específicos para la jurisdicción y las obligaciones, actividades y productos del auditado;
— requisitos de las partes interesadas relevantes a la disciplina específica;
— fundamentos de la disciplina y aplicación suficiente de métodos, técnicas, procesos y prácticas técnicas y de negocio específicas a la disciplina, que permitan al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiadas;
— conocimiento específico a la disciplina relacionado con el sector particular, la naturaleza de las operaciones o lugar de trabajo que está siendo auditado que sea suficiente para que el auditor evalúe las actividades, procesos y productos (bienes y servicios) del auditado;
— principios de gestión del riesgo, métodos y técnicas relevantes a la disciplina y el sector, de manera que el auditor pueda evaluar y controlar los riesgos asociados con el programa de auditoría.

NOTA El anexo A provee una guía y ejemplos ilustrativos de conocimiento y habilidades específicas a la disciplina de los auditores.

7.2.3.4 Conocimiento genérico y habilidades del líder del equipo auditor

Los líderes de equipo auditor deberían tener conocimiento y habilidades adicionales para manejar y proveer liderazgo al equipo de auditoría, a fin de facilitar la realización efectiva y eficiente de la auditoría. Un líder de equipo auditor debería tener el conocimiento y habilidades necesarias para hacer lo siguiente:

a) hacer un balance entre las fortalezas y debilidades de los miembros del equipo auditor;

b) desarrollar relaciones de trabajo armoniosas entre los miembros del equipo auditor;

c) gestionar el proceso de auditoría, incluyendo:
— planear la auditoría y hacer uso efectivo de los recursos durante la auditoría;
— manejar la incertidumbre de alcanzar los objetivos de auditoría;
— proteger la salud y seguridad de los miembros del equipo auditor durante la auditoría, incluyendo el asegurar cumplimiento de los auditores con los requisitos relevantes de salud y seguridad;
— organizar y dirigir a los miembros del equipo auditor;
— proveer dirección y guía a los auditores en entrenamiento;
— prevenir y resolver conflictos, de ser necesario;

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

e) conducir al equipo auditor hacia alcanzar las conclusiones de auditoría;
f) preparar y completar el reporte de auditoría.

7.2.3.5 Conocimiento y habilidades para auditor sistemas de gestión que tratan múltiples disciplina

Los auditores que buscan participar como miembros de un equipo auditor durante la auditoría de sistemas de gestión que tratan múltiples disciplinas deberían tener la competencia necesaria para auditar al menos una de las disciplinas de sistemas de gestión y una comprensión de la interacción y sinergia entre los diferentes sistemas de gestión.

Los líderes de equipo auditor que llevan a cabo auditorías a sistemas de gestión que tratan múltiples disciplinas deberían entender los requisitos de cada una de las normas de sistemas de gestión y reconocer los límites de su conocimiento y habilidades en cada una de las disciplinas.

7.2.4 Logro de competencias de auditor

El conocimiento y habilidades de auditor se pueden adquirir usando una combinación de lo siguiente:
— educación formal/entrenamiento y experiencia que contribuye al desarrollo de conocimiento y habilidades en la disciplina y sector de sistema de gestión que el auditor busca auditar;
— programas de entrenamiento que cubren conocimiento genérico y habilidades de auditor;
— experiencia en una posición técnica, gerencial o profesional relevante que involucres el ejercicio de juicio, toma de decisiones, solución de problemas y comunicación con gerentes, profesionales, pares, clientes y otras partes interesadas;
— experiencia de auditoría adquirida bajo la supervisión de un auditor en la misma disciplina.

7.2.5 Líderes de equipo auditor

Un líder de equipo auditor debería haber adquirido experiencia adicional de auditoría para desarrollar el conocimiento y habilidades descritas en 7.2.3. Esta experiencia adicional debería haber sido ganada al trabajar bajo la dirección y guía de un líder de equipo auditor diferente.

7.3 Establecimiento de criterios de evaluación del auditor

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

7.4 Selección del método apropiado de evaluación del auditor

La evaluación debería ser realizada usando dos o más de los métodos seleccionados de aquellos que aparecen en la Tabla 2. Al usar la Tabla 2 se debe tener en cuenta lo siguiente:

— los métodos presentados representan un rango de opciones y pueden no aplicar en todas las situaciones;
— los varios métodos presentados pueden diferir en su confiabilidad;
— se debería usar una combinación de métodos para asegurar un resultado que sea objetivo, consistente, justo y confiable.

Tabla 2 — Posibles Métodos de Evaluación

Método de Evaluación	Objetivos	Ejemplos
Revisión de registros	Verificar los antecedentes del auditor	Análisis de registros de educación, entrenamiento, empleo, credenciales profesionales y experiencia en auditoría
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 los atributos personales y las habilidades de comunicación, para verificar la información y examinar los conocimientos, y para obtener información adicional	Entrevistas personales
Observación	Evaluar los atributos personales y la aptitud para aplicar los conocimientos y habilidades	Actuación, testificación de auditorías, desempeño en el trabajo
Examen	Evaluar las cualidades personales, los conocimientos y habilidades, y su aplicación	Exámenes orales y escritos, exámenes psicotécnicos
Revisión después de la auditoría	Proveer información sobre el desempeño del auditor durante las actividades de auditoría, identificar fortalezas y debilidades	Revisión del reporte de auditoría, entrevistas con el líder del equipo auditor, con el equipo auditor y, si es adecuado, retroalimentación del auditado.

7.5 Realización de la evaluación del auditor

La información recopilada de la persona debería compararse contra los criterios establecidos en 7.2.3. Cuando una persona que se espera que participe en el programa de auditoría no cumple con los criterios, se debería tomar entrenamiento, trabajo o experiencia de auditoría adicional y se debería llevar a cabo una re-evaluación posterior.

7.6 Mantenimiento y mejora de la competencia del auditor

Los auditores y los líderes de equipo auditor deberían mejorar continuamente su competencia. Los auditores deberían mantener su competencia de auditoria a través de la participación regular en auditorías a sistemas de gestión y el continuo desarrollo profesional. El continuo desarrollo profesional involucra el mantenimiento y mejora de la competencia. Esto se puede lograr a través de medios tales como experiencia laboral adicional o entrenamiento, estudio, preparación, asistencia a reuniones, seminarios y conferencias u otras actividades relevantes.

La persona que gestiona el programa de auditoría debería establecer mecanismos apropiados para la evaluación continua del desempeño de los auditores y líderes de equipo auditor.

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

— cambios en las necesidades del individuo y la organización responsable de realizar la auditoría;
— la práctica de auditoría;
— normas y otros requisitos relevantes.

Anexo A
(informativo)

Guía y ejemplos ilustrativos de conocimiento y habilidades de auditores específicas a una disciplina

A.1 Generalidades

Este anexo provee ejemplos genéricos de conocimiento y habilidades de auditores de sistemas de gestión específicas a una disciplina, que buscan servir como guía para ayudar a la persona que gestiona el programa de auditoría a seleccionar o evaluar los auditores.

Es posible desarrollar otros ejemplos de conocimiento y habilidades de auditor específicas a una disciplina. Se sugiere que, cuando sea posible, tales ejemplos sigan la misma estructura general a fin de asegurar comparabilidad.

A.2 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de seguridad de transporte

El conocimiento y habilidades relacionadas con la gestión de seguridad de transporte y la aplicación de métodos, técnicas, procesos y prácticas de gestión de seguridad de transporte debería ser suficiente para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Los siguientes son ejemplos:
— terminología de gestión de seguridad;
— comprensión del enfoque de sistema seguro;
— evaluación y mitigación de riesgos;
— análisis de factores humanos relacionados con la gestión de seguridad en transporte;
— comportamiento humano e interacción;
— interacción de humanos, máquinas, procesos y el ambiente de trabajo;
— peligros potenciales y otros factores del lugar de trabajo que afectan la seguridad;
— métodos y prácticas para investigación de incidentes y monitoreo de desempeño en seguridad;
— evaluación de incidentes y accidentes operacionales;
— desarrollo de medidas y mediciones proactivas y reactivas de desempeño.

NOTA Para información adicional, vea la futura ISO 39001 desarrollada por ISO/PC 241 sobre sistemas de gestión de seguridad de tráfico en carreteras.

A.3 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión ambiental

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— terminología ambiental;
— mediciones y estadísticas ambientales;
— ciencia de medición y técnicas de monitoreo;
— interacción de ecosistemas y biodiversidad;
— medios ambientales (ej. aire, agua, suelo, fauna, flora);
— técnicas para determinar riesgo (ej. evaluación de aspectos/impactos ambientales, incluyendo métodos para evaluación de significancia);
— evaluación de ciclo de vida;
— evaluación de desempeño ambiental;
— prevención y control de la contaminación (ej. mejores técnicas disponibles para control de contaminación y eficiencia energética);
— reducción en la fuente, minimización de residuos, re-uso, reciclado y prácticas y procesos de tratamiento;
— uso de sustancias peligrosas;
— conteo y gestión de emisión de gases de invernadero;
— manejo de recursos naturales (ej. combustible fósil, agua, flora y fauna, suelo);
— diseño ambiental;
— reporte y divulgación ambiental;
— administración de productos;
— tecnologías renovables y de bajo carbono.

NOTA Para información adicional, vea las normas relacionadas desarrolladas por ISO/TC 207 sobre gestión ambiental.

A.4 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de calidad

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— terminología relacionada con calidad, gestión, organización, proceso y producto, características, conformidad, documentación, procesos de auditoría y de medición;
— enfoque al cliente, procesos relacionados con el cliente, monitoreo y medición de satisfacción del cliente, manejo de quejas, código de conducta, resolución de disputas;
— liderazgo – rol de la alta gerencia, gestión para el éxito sostenido de una organización – el enfoque de gestión de la calidad, alcanzando beneficios económicos y financieros a

través de la gestión de la calidad, sistemas de gestión de calidad y modelos de excelencia;
— participación de las personas, factores humanos, competencia, entrenamiento y toma de conciencia;
— enfoque por procesos, análisis de procesos, técnicas de capacidad y control, métodos de tratamiento de riesgos;
— enfoque de sistemas para la gestión (relación de sistemas de gestión de calidad, sistemas de gestión de calidad y otros enfoques de sistemas de gestión, documentación de sistema de gestión de calidad), tipos y valor, proyectos, planes de calidad, gestión de configuración;
— mejora continua, innovación y aprendizaje;
— enfoque en hechos para toma de decisiones, técnicas de evaluación de riesgos (identificación, análisis y evaluación de riesgos), evaluación de gestión de calidad (auditoría, revisión y auto-evaluación), técnicas de monitoreo y medición, requisitos para procesos de medida y equipo de medición, análisis de causa raíz, técnicas estadísticas;
— características de procesos y productos, incluyendo servicios;
— relaciones mutuamente beneficiosas con los proveedores, requisitos del sistema de gestión de calidad y requisitos de productos, requisitos particulares para gestión de calidad en diferentes sectores.

NOTA Para información adicional, vea las normas relacionadas desarrolladas por ISO/TC 176 sobre gestión de calidad.

A.5 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de registros

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— registros, procesos de gestión de registros y sistemas de gestión para terminología de registros;
— desarrollo de medidas y mediciones de desempeño;
— prácticas de investigación y evaluación de registros a través de entrevistas, observación y validación;
— análisis de muestra de registros creados en procesos de negocios. Características clave de registros, sistemas de registros, procesos y control de registros;
— evaluación de riesgos (ej. evaluación de riesgos a través de falla en la creación, mantenimiento y control de registros adecuados para los procesos de negocio de la organización);
— el desempeño y adecuación de los procesos para crear, capturar y controlar registros;
— valuación de la adecuación y desempeño de sistemas de registros (incluidos sistemas de negocio para crear y controlar registros), la idoneidad de las herramientas tecnológicas usadas, así como de las instalaciones y equipo establecido;
— evaluación de los diferentes niveles de competencia en gestión de registros requerida en toda la organización y la evaluación de dicha competencia;
— significancia del contenido, contexto, estructura, representación e información de control (metadatos) requeridos para definir y gestionar sistemas de registros;
— métodos para desarrollar instrumentos específicos a los registros;
— tecnologías usadas para la creación, captura, conversión y migración y preservación a largo plazo de registros electrónicos/digitales;

— identificación y significancia de la documentación de autorización para procesos de registros.

NOTA Para información adicional, vea las normas relacionadas desarrolladas por ISO/TC 46/SC 11 sobre gestión de registros.

A.6 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de flexibilidad, seguridad, preparación y continuidad

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— procesos, ciencia y tecnología subyacentes a la gestión de flexibilidad, seguridad, preparación, respuesta, continuidad y recuperación;
— métodos de monitoreo y recopilación de inteligencia;
— gestión del riesgo de eventos perjudiciales (anticipar, evitar, prevenir, proteger, mitigar, responder y recuperarse de un evento perjudicial);
— evaluación de riesgo (identificación y valoración de actives; e identificación, análisis y evaluación de riesgos) y análisis de impacto (relacionados con activos humanos, físicos e intangibles, así como con el ambiente);
— tratamiento de riesgos (medidas adaptativas, proactivas y reactivas);
— métodos y prácticas para integridad y sensibilidad de la información;
— métodos para seguridad del personal y protección de personas;
— métodos y prácticas para protección de actives y seguridad física;
— métodos y prácticas para prevención, disuasión y gestión de seguridad;
— métodos y prácticas para mitigación de incidentes, respuesta y manejo de crisis;
— métodos y prácticas para gestión de continuidad, emergencia y recuperación;
— métodos y prácticas para monitoreo, medición y reporte de desempeño (incluyendo metodologías de ejercicio y prueba).

NOTA Para información adicional, vea las normas relacionadas desarrolladas por ISO/TC 8, ISO/TC 223 e ISO/TC 247 sobre gestión de la flexibilidad, seguridad, preparación y continuidad.

A.7 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de seguridad de la información

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— lineamientos de normas como ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005;
— identificación y evaluación de requisitos de clientes y partes interesadas;

— las leyes y regulaciones que tratan el tema de seguridad de la información (ej. propiedad intelectual; contenido, protección y retención de registros organizacionales; protección de datos y privacidad; regulación de controles criptográficos; anti-terrorismo; comercio electrónico; firmas digitales y electrónicas; vigilancia del lugar de trabajo; ergonomía del lugar de trabajo; intercepción de telecomunicaciones y monitoreo de datos(ej. e-mail), abuso de computador, recolección de evidencia electrónica, pruebas de penetración, etc.;
— procesos, ciencia y tecnología subyacente a la gestión de seguridad de la información;
— evaluación de riesgos (identificación, análisis y evaluación) y tendencias en tecnología, amenazas y vulnerabilidades;
— gestión de riesgo de seguridad de la información;
— métodos y prácticas para control de seguridad de información (electrónica y física);
— métodos y prácticas para integridad y sensibilidad de información;
— métodos y prácticas para medir y evaluar la efectividad del sistema de gestión de seguridad de la información y controles asociados;
— métodos y prácticas para medir, monitorear y registrar el desempeño (incluyendo pruebas, auditorías y revisiones).

NOTA Para información adicional vea las normas asociadas desarrolladas por ISO/IEC JTC 1/SC 27 sobre gestión de seguridad de la información
.

A.8 Ejemplo ilustrativo de conocimiento y habilidades de auditor específicas a una disciplina en gestión de seguridad y salud ocupacional

A.8.1 Conocimiento general y habilidades

El conocimiento y habilidades relacionadas a la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos a esta disciplina deberían ser suficientes para permitir al auditor examinar el sistema de gestión y generar hallazgos y conclusiones de auditoría apropiados.

Algunos ejemplos son:
— identificación de peligros, incluyendo aquellos y otros factores que afectan el desempeño humano en el lugar de trabajo (tales como factores físicos, químicos y biológicos, así como género, edad, discapacidad u otros factores psicológicos, psicosociales o de salud);
— evaluación de riesgos, determinación de controles y comunicación de riesgos [la determinación de controles debería estar basada en la “jerarquía de controles” (ver OHSAS 18001:2007, 4.3.1)];
— la evaluación de factores de salud y humanos (incluyendo factores psicológicos y psicosociales) y los principios para evaluarlos;
— método para el monitoreo de exposición y evaluación de riesgos de seguridad y salud ocupacional (incluyendo aquellos que surgen de los factores humanos mencionados arriba o relacionados con la higiene ocupacional) y estrategias relacionadas para eliminar o minimizar dichas exposiciones;
— comportamiento humano, interacciones persona a persona y la interacción de humanos con las máquinas, procesos y el ambiente de trabajo (incluyendo lugar de trabajo, ergonomía y principios de diseño seguro, información y tecnologías de comunicación;

— la evaluación de los diferentes tipos y niveles de competencia en seguridad y salud ocupacional requeridos en la organización y la evaluación de dicha competencia;
— métodos para animar la participación de los empleados;
— métodos para animar el bienestar y auto-responsabilidad de los empleados (en relación a fumar, drogas, problemas de peso, ejercicio, stress, comportamiento agresivo, etc.), tanto durante las horas de trabajo como en sus vidas privadas;
— el desarrollo, uso y evaluación de medidas y mediciones de desempeño reactive y proactivo;
— los principios y prácticas para identificar situaciones potenciales de emergencia y para la planeación, prevención y recuperación de emergencias;
— métodos para investigación y evaluación de incidentes (incluyendo accidentes y enfermedades relacionadas con el trabajo);
— la determinación y uso de información relacionada con salud (incluyendo datos de monitoreo de exposición y enfermedades relacionadas con el trabajo) – pero dando atención especial a la confidencialidad de ciertos aspectos de tal información;
— comprensión de información médica (incluyendo terminología médica suficiente para entender datos relacionados con la prevención de heridas y enfermedades);
— sistemas de valores de “límites de exposición ocupacional”;
— métodos para monitoreo y reporte de desempeño de seguridad y salud ocupacional;
— comprensión de requisitos legales y otros requisitos relevantes a la seguridad y salud ocupacional suficiente para permitir que el auditor evalúe el sistema de gestión de seguridad y salud ocupacional.

A.8.2 Conocimiento y habilidades relacionadas con el sector que está siendo auditado

Conocimiento y habilidades relacionadas con el sector que está siendo auditado deberían ser suficientes para permitir que el auditor examine el sistema de gestión desde el contexto del sector y genere hallazgos y conclusiones de auditoría apropiadas

Algunos ejemplos son:
— procesos, equipos, materias primas, sustancias peligrosas, ciclos de proceso, mantenimiento, logística, organización del flujo de trabajo, prácticas de trabajo, programación de turnos, cultura organizacional, liderazgo, comportamiento y otros temas específicos a la operación o sector;
— riesgos y peligros típicos para el sector, incluyendo factores humanos y de salud.

NOTA Para información adicional ver las normas relacionadas desarrolladas por el grupo de proyecto OHSAS sobre gestión de seguridad y salud ocupacional.

Anexo B
(Informativo)

Guía adicional para los auditores sobre planeación y realización de auditorías

B.1 Aplicación de métodos de auditoría

Una auditoría puede ser realizada usando un amplio rango de métodos de auditoría. En este anexo se puede encontrar una explicación de los métodos de auditoría comúnmente usados. Los métodos de auditoría escogidos para una auditoría dependen de los objetivos, alcance y criterios de auditoría definidos, así como de la duración y ubicación. También se debería tener en cuenta la competencia del auditor disponible y cualquier incertidumbre que surja de la aplicación de los métodos de auditoría. La aplicación de una variedad y combinación de diferentes métodos de auditoría puede optimizar la eficiencia y efectividad del proceso de auditoría y su resultado.

El desarrollo de una auditoría involucra una interacción entre individuos con el sistema de gestión que está siendo auditado y la tecnología usada para realizar la auditoría. La Tabla B.1 provee ejemplos de métodos de auditoría que pueden ser usados, solos o combinados, a fin de alcanzar los objetivos de auditoría. Si una auditoría involucra el uso de un equipo de auditores con múltiples miembros, se pueden usar tanto métodos en sitio como remotos de manera simultanea.

NOTA La cláusula B.6 da información adicional sobre visitas a sitio.

Tabla B.1 — Métodos de auditoría aplicables

Grado de interacción entre el auditor y el auditado	Ubicación del auditor	
	En sitio	**Remota**
Interacción humana	Conducir entrevistas. Completar listas de verificación y cuestionarios con la participación del auditado. Revisión documental con participación del auditado. Muestreo.	A través de medios de comunicación interactiva: — entrevistas; — completar listas de chequeo y cuestionarios; — revisión documental con participación del auditado.
Sin interacción humana	Revisión documental (ej. registros, análisis de datos). Observación del trabajo realizado. Visita a sitio. Completar listas de verificación. Muestreo (ej. productos).	Revisión documental (ej. registros, análisis de datos). Observación de trabajo a través de medios de vigilancia, teniendo en cuenta requisitos legales y sociales. Análisis de datos.
Las actividades de auditoría en sitio son llevadas a cabo en las instalaciones del auditado. Las actividades de auditoria remota son desarrolladas en otro sitio diferente a las instalaciones del auditado, independientemente de la distancia. Las actividades interactivas de auditoría involucran interacción entre el personal del auditado y el equipo auditor. Las actividades no interactivas de auditoría no involucran interacción humana con personas que representan al auditado pero sí con equipo, instalaciones y documentación.		

La responsabilidad de la aplicación efectiva de los métodos de auditoría durante cualquier auditoría dada, en la etapa de planeación sigue siendo de la persona que gestiona el programa de auditoría o del auditor líder. El líder del equipo auditor tiene la responsabilidad de realizar las actividades de auditoría.

La viabilidad de actividades de auditoría remota puede depender del nivel de confianza entre el auditor y el personal del auditado.

A nivel del programa de auditoria, éste debería asegurar que el uso de métodos de aplicación de auditoría en sitio y remoto es adecuado y equilibrado, a fin de asegurar y logro satisfactorio de los objetivos del programa.

B.2 Revisión documental

Los auditores deberían considerar si:

— la información entregada en los documentos es:
  — completa (todo el contenido esperado se encuentra en el documento);
  — correcta (el contenido está conforme con otras fuentes confiables tales como normas y regulaciones);
  — consistente (el documento es consistente con sigo mismo y con documentos relacionados);
  — actual (el contenido está actualizado);

— los documentos que están siendo revisados cubren el alcance de auditoría y proveen suficiente información para soportar los objetivos de la auditoría;
— el uso de tecnologías de información y comunicación, dependiendo de los métodos de auditoría, promueve una realización eficiente de la auditoría: se debe tener cuidado específico para seguridad de la información debido a regulaciones aplicables sobre protección de datos (en particular para información que está fuera del alcance de la auditoría pero que está contenida en el documento).

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

B.3 Muestreo

B.3.1 Generalidades

En auditoría, el muestreo tienen lugar cuando no resulta práctico o no es efectivo desde el punto de vista de costos examinar toda la información disponible durante una auditoría; ej. los registros son muy numerosos o demasiado dispersos geográficamente para justificar el examen de cada uno de los elementos dentro de la población. El muestreo en auditoría de una larga población es el proceso de seleccionar menos del 100% de los elementos dentro del total de datos disponibles (población) para obtener y evaluar la evidencia acerca de algunas características de dicha población a fin de llegar a una conclusión que aplique para toda la población.

El objetivo del muestreo en auditoría es proveer información tal que el auditor tenga la confianza de que se podrán alcanzar los objetivos de la auditoría.

El riesgo asociado con el muestreo es que las muestras pueden no ser representativas de la población de la cual son seleccionadas, y por lo tanto la conclusión del auditor puede estar sesgada y ser diferente de aquella que se alcanzaría si se examinara toda la población. Puede haber otros riesgos dependiendo de la variabilidad dentro de la población a ser muestreada y el método utilizado.

El muestreo en auditoría típicamente involucra los siguientes pasos:
— establecer los objetivos del plan de muestreo;
— seleccionar el grado y composición de la población a ser muestreada;
— seleccionar el método de muestreo;
— determinar el tamaño de muestra a tomar;
— llevar a cabo la actividad de muestreo;
— compilar, evaluar, reportar y documentar resultados.

Al realizar el muestreo, se debería prestar atención a la calidad de los datos disponibles ya que un muestreo insuficiente y datos incorrectos no entregarán un resultado útil. La selección de una muestra apropiada debería estar basada tanto en el método de muestreo como en el tipo de datos requeridos, ej. para inferir un patrón de comportamiento particular en una población.

El reporte sobre la muestra seleccionada podría tener en cuenta el tamaño de la muestra, el método de selección y estimados hechos sobre la base de la muestra y el nivel de confianza.

En las auditorías se puede usar ya sea el muestreo basado en juicio (ver B.5.2) o el muestreo estadístico (ver B.5.3).

B.3.2 Muestreo basado en Juicio

El muestreo basado en juicio confía en el conocimiento, habilidades y experiencia del equipo auditor (Ver Capítulo 7)

Para realizar un muestreo basado en juicio, se puede tener en cuenta lo siguiente:
— experiencia previa de auditoría dentro del alcance de la auditoría;
— complejidad de los requisitos (incluyendo requisitos legales) para alcanzar los objetivos de la auditoría;
— complejidad e interacción de los procesos de la organización y los elementos del sistema de gestión;
— grado de cambio en la tecnología, factor humano o sistema de gestión;
— áreas clave de riesgo previamente identificadas y áreas de mejora;
— salidas para el monitoreo de los sistemas de gestión.

Un inconveniente del muestreo basado en juicio es que puede no haber un estimado estadístico sobre el efecto de incertidumbre en los hallazgos y conclusiones de auditoría alcanzados.

B.3.3 Muestreo Estadístico

Si se toma la decisión de usar muestreo estadístico, el plan de muestreo debería estar basado en los objetivos de la auditoría y en lo que se conoce acerca de las características de la población general de la cual se están tomando las muestras.

— El muestreo estadístico usa un proceso de selección de muestra basado en la teoría de probabilidad. El muestreo basado en atributos se usa cuando solo hay dos resultados posibles de muestra para cada muestra (ej. correcto/incorrecto o pasó/falló). El muestreo basado en variable se usa cuando los resultados de muestra se dan en un rango continuo.

— El plan de muestreo debería tener en cuenta si hay la probabilidad de que el resultado que se está examinando sea basado en atributos o basado en variable. Por ejemplo, al evaluar conformidad de los formularios completados con los requisitos establecidos en un procedimiento, se pude usar un enfoque de muestreo basado en atributos. Al examinar la ocurrencia de incidentes de seguridad en alimentos o el número de brechas de seguridad, un enfoque basado en variable probablemente sería más apropiado.

— Los elementos clave que afectarán el plan de muestreo de auditoría son:
  — el tamaño de la organización;
  — el número de auditores competentes;
  — la frecuencia de las auditorías durante el año;
  — el tiempo de una auditoría individual;
  — cualquier nivel de confianza requerido externamente.

— Cuando se desarrolla un plan de muestreo estadístico, el nivel de riesgo de muestreo que el auditor está dispuesto a aceptar es una consideración importante. Esto a menudo es conocido como el nivel de confianza aceptado. Por ejemplo, un riesgo de muestreo de 5 % corresponde a un nivel de confianza aceptado de 95%. Un riesgo de muestreo de 5% significa que el auditor está dispuesto a aceptar el riesgo de que 5 de cada 100 (o 1 de 20) muestras examinadas no reflejará los valores reales que se encontrarían si toda la población fuera examinada.

— Cuando se usa el muestreo estadístico, los auditores deberían documentar apropiadamente el trabajo realizado. Esto debería incluir una descripción de la población que se quiere muestrear, los criterios de muestreo usados para la evaluación (ej. qué es una muestra aceptable), los parámetros estadísticos y los métodos utilizados, el número de muestras y los resultados obtenidos.

B.4 Preparación de documentos de trabajo

Al preparar documentos de trabajo, el equipo auditor debería considerar las preguntas que se encuentran a continuación para cada documento.

a) ¿Qué registro de auditoría será creado al usar este documento de trabajo?
b) ¿Qué actividad de auditoría está relacionada con este documento de trabajo en particular?

c) ¿Quién será el usuario de este documento de trabajo?
d) ¿Qué información es necesaria para preparar este documento de trabajo?

Para auditorías combinadas, los documentos de trabajo deberían ser desarrollados para evitar la duplicación de actividades de auditoría al:
— agrupar requisitos similares de diferentes criterios;
— coordinar el contenido de las listas de verificación y cuestionarios relacionados.

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

B.5 Selección de fuentes de información

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

— entrevistas con empleados y otras personas;
— observación de actividades y el ambiente y condiciones que rodean el trabajo;
— documentos, tales como políticas, objetivos, planes, procedimientos, normas, instrucciones, licencias y permisos, especificaciones, dibujos, contraltos y órdenes;
— registros, tales como registros de inspección, actas de reunión, reportes de auditoría, registros de programa de monitoreo y los resultados de las mediciones;
— resúmenes de datos, análisis e indicadores de desempeño;
— información sobre los planes de muestreo del auditado y sobre los procedimientos para los procesos de control de muestreo y de medición;
— reportes de otras fuentes, ej. retroalimentación de clientes, encuestas y mediciones externas, y otra información relevante de partes externas y calificación de proveedores;
— bases de datos y sitios web;
— simulación y modelado.

B.6 Guía sobre visitas a instalaciones del auditado

Para minimizar la interferencia entre las actividades de auditoría y los procesos de trabajo del auditado y a fin de asegurar la salud y seguridad del equipo auditor durante una visita, se debería tener en cuenta lo siguiente:

a) planear la visita:
— asegurar permiso y acceso a aquellos sitios de las instalaciones del auditado que se van a visitar, de acuerdo con el alcance de la auditoría;
— proveer información adecuada a los auditores (ej. reunión informativa) en materia de seguridad, salud (ej. cuarentena), salud ocupacional y normas culturales para la visita, incluyendo vacunación y autorizaciones solicitadas y recomendadas, si aplican;
— confirmar con el auditado que cualquier equipo de protección personal (EPP) requerido estará disponible para el equipo auditor, si aplica;
— excepto para auditorías no programadas y auditorías ad hoc, asegurar que el personal que se va a visitar esté informado acerca de los objetivos y alcance de la auditoría;

b) actividades en sitio:

— evitar cualquier interrupción innecesaria de los procesos operacionales;
— asegurar que el equipo auditor está usando adecuadamente el EPP;
— asegurar que los procedimientos de emergencia son comunicados (ej. salidas de emergencia, puntos de encuentro);
— programar la comunicación para minimizar la interrupción;
— adaptar el tamaño del equipo auditor y el número de guías y observadores de acuerdo con el alcance de la auditoría, a fin de evitar interferencia con los procesos operacionales tanto como sea posible;
— no tocar o manipular ningún equipo, a menos que le sea explícitamente permitido, aunque sea competente o tenga licencia para hacerlo;
— si ocurre un incidente durante la visita a sitio, el líder del equipo auditor debería revisar la situación con el auditado y, si es necesario, con el cliente de auditoría y debería llegar a un acuerdo respecto a si la auditoría debería ser interrumpida, re-programada o continuada;
— si va a tomar fotos o video, pida autorización de la gerencia con anticipación y tenga en cuenta los temas de seguridad y confidencialidad; evite tomar fotografías de personas individuales sin su permiso;
— al sacar copias de documentos de cualquier clase, pida permiso con antelación y tenga en cuenta los temas de confidencialidad y seguridad;
— al tomar notas, evite recolectar información personal a menos que esto sea requerido por los objetivos o criterios de la auditoría.

B.7 Realización de entrevistas

Las entrevistas son uno de los medios importantes para recolectar información y deberían ser llevadas a cabo de manera tal que sean adaptadas a la situación y la persona entrevistada, ya sea frente a frente o por otros medios de comunicación.

Sin embargo, el auditor debería tener en cuenta lo siguiente:
— las entrevistas se deberían realizar a personas en niveles y funciones apropiadas que lleven a cabo actividades o tareas que se encuentren dentro del alcance de la auditoría;
— las entrevistas normalmente deberían ser realizadas durante horas normales de trabajo cuando sea posible, en el sitio habitual de trabajo de la persona entrevistada;
— busque tranquilizar a la persona que va a entrevistar antes y durante la entrevista;
— se debería explicar la razón de la entrevista y cualquier nota tomada;
— las entrevistas pueden ser iniciadas solicitando a las personas que describan su trabajo;
— selección cuidadosa del tipo de pregunta usada (ej., abierta, cerrada, conducente);
— los resultados de la entrevista deberían ser resumidos y revisados con la persona entrevistada;
— se debería agradecer a la persona entrevistada por su participación y cooperación.

B.8 Hallazgos de auditoría

B.8.1 Determinación de hallazgos de auditoría

Al determinar los hallazgos de auditoría, se debería considerar lo siguiente:
— seguimiento de registros y conclusiones de auditorías previas;
— requisitos del cliente de auditoría;
— hallazgos que exceden la práctica normal, u oportunidades de mejora;
— tamaño de la muestra;
— categorización (de haberla) de los hallazgos de auditoría;

B.8.2 Registro de conformidades

Para registros de conformidad, se debería tener en cuenta lo siguiente:
— identificación de los criterios de auditoría contra los cuales se muestra la conformidad;
— evidencia de auditoria para soportar la conformidad;
— declaración de conformidad, si aplica.

B.8.3 Registro de no conformidades

Para registros de no conformidad, se debería tener en cuenta lo siguiente:
— descripción o referencia a los criterios de auditoría;
— declaración de no conformidad;
— evidencia de auditoría;
— hallazgos de auditoría relacionados, si aplica.

B.8.4 Tratamiento de hallazgos relacionados con múltiples criterios

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

Dependiendo de lo acordado con el cliente de auditoría, el auditor puede levantar:
— hallazgos separados para cada criterio; o
— un único hallazgo, combinando las referencias a múltiples criterios.

Dependiendo de los acuerdos con el cliente de auditoría, el auditor puede guiar al auditado sobre como responder a dichos hallazgos.

Bibliografía

[1] ISO 2859-4, *Procedimientos de muestreo para inspección por atributos — Parte 4: Procedimientos para evaluación de niveles de calidad declarados.*
[2] ISO 9000:2005, *Sistemas de Gestión de Calidad – Fundamentos y vocabulario*
[3] ISO 9001, *Sistemas de gestión de calidad - Requisitos*
[4] ISO 14001, *Sistemas de gestión ambiental – Requisitos y guía de uso*
[5] ISO 14050, *Gestión ambiental -Vocabulario*
[6] ISO/IEC 17021:2011, *Evaluación de conformidad — Requisitos para entes que proveen auditoría y certificación a sistemas de gestión.*
[7] ISO/IEC 20000-1, *Tecnología de información — Gestión de servicio — Parte 1: Requisitos de sistema de Gestión de Servicio*
[8] ISO 22000, *Sistemas de gestión de seguridad alimentaria – Requisitos para una organización dentro de la cadena alimentaria*
[9] ISO/IEC 27000, *Tecnología de información — Técnicas de seguridad — sistemas de gestión de seguridad de la información — Generalidades y vocabulario*
[10] ISO/IEC 27001, *Tecnología de información — Técnicas de seguridad —Sistemas de gestión de seguridad de la información - Requisitos*
[11] ISO/IEC 27002, *Tecnología de información — Técnicas de seguridad — Código de práctica para gestión de seguridad de la información*
[12] ISO/IEC 27003, *Tecnología de información – Técnicas de seguridad — Guía para la implementación de sistemas de gestión de seguridad de la información*
[13] ISO/IEC 27004, *Tecnología de información — Técnicas de seguridad — Gestión de seguridad de la información — Medición*
[14] ISO/IEC 27005, *Tecnología de información — Técnicas de seguridad — Gestión de riesgos de seguridad de la información*
[15] ISO 28000, *Especificación para sistemas de gestión de seguridad para la cadena de suministro*
[16] ISO 303011), *Información y documentación — Sistema de gestión para registros — Requisitos*
[17] ISO 31000, *Gestión del Riesgo — Principios y lineamientos*
[18] ISO 390012), *Sistemas de gestión de seguridad en la vía – Requisitos y guía de uso*
[19] ISO 50001, *Sistema de gestión de energía – Requisitos con guía de uso*
[20] ISO Guía 73:2009, *Gestión de Riesgo - Vocabulario*
[21] OHSAS 18001:2007, *Sistemas de Gestión de seguridad y salud ocupacional - Requisitos*
[22] *ISO 9001* Papeles de *Grupo de Prácticas de Auditoría* disponibles en:
www.iso.org/tc176/ISO9001AuditingPracticesGroup
[23] ISO 19011 lineamientos adicionales disponibles en:
www.iso.org/19011auditing