www.ingecal.cat ingecal@ingecal.cat Tel. 93 237 83 90

UNE-EN ISO 19011. Directrices para la auditoría de los sistemas de gestión

Se acaba de publicar la tercera edición de la norma UNE-EN ISO 19011:2018, tras las versiones anteriores de 2002 y 2011.

Se trata de una guía que especifica las orientaciones a aplicar en la gestión de un programa de auditoría, tanto internas (primera parte) como externas (segunda parte). Es aplicable a todas las organizaciones que necesitan planificar y realizar auditorías internas o externas de sistemas de gestión, o gestionar un programa de auditoría.

Las principales novedades de esta nueva versión son:

- Incorporación del enfoque basado en riesgos en la gestión del programa de auditoría;
- Incorporación de nuevos requisitos de competencia genérica para los auditores;
- Ampliación del anexo A para proporcionar orientación sobre la auditoría de conceptos como el contexto de la organización, el liderazgo y el compromiso, las auditorías virtuales, el cumplimiento y la cadena de suministro.

Auditorías: físicas, en remoto o virtuales

Las auditorías pueden llevarse a cabo in situ o remotamente, o como una combinación de ambos. El uso de estos métodos tiene que estar adecuadamente equilibrado, basándose, entre otros, en la consideración de los riesgos y oportunidades asociados.

Las ubicaciones pueden ser **físicas** o **virtuales**. Las auditorías virtuales se realizan cuando una organización desempeña trabajo o proporciona un servicio usando un entorno en línea que permite a las personas con independencia de la ubicación física, ejecutar procesos (por ejemplo, la intranet de la empresa, “uso de la nube”. Las auditorías **remotas** hacen referencia al uso de tecnología para recopilar información, entrevistar a un auditado, etc., cuando los métodos “cara a cara” no son posibles o deseables.

No conformidades

Las no conformidades pueden clasificarse dependiendo del contexto de la organización y de sus riesgos. Esta clasificación puede ser cuantitativa (por ejemplo, de uno a cinco) y cualitativa (por ejemplo, menor, mayor). Deberían revisarse con el auditado para reconocer que la evidencia de la auditoría es exacta y que las no conformidades se han comprendido. Se debería realizar todo el esfuerzo posible para resolver cualquier opinión divergente relativa a las evidencias o a los hallazgos de la auditoría. Las cuestiones no resueltas deberían registrarse en el informe de la auditoría.

Definiciones

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Criterios de auditoría: Conjunto de requisitos usados como referencia frente a la cual se compara la evidencia objetiva.

Evidencia objetiva: Datos que respaldan la existencia o veracidad de algo.

Evidencia de la auditoría: Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable.

Hallazgos de la auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

Conclusiones de la auditoría: Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

www.ingecal.cat ingecal@ingecal.cat Tel. 93 237 83 90

Principios de auditoría

Los principios de auditoría permiten 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.

Gestión de un programa de auditoría

Define los criterios para gestionar globalmente las auditorías internas de una organización (aplicable a empresas organizaciones con varios auditores).

www.ingecal.cat ingecal@ingecal.cat Tel. 93 237 83 90

Las etapas de una auditoría son:

Anexo A

A.1 Enfoque a procesos para la auditoría

El uso de un "enfoque a procesos" es un requisito para todas las normas de sistemas de gestión de ISO de acuerdo con las Directivas ISO/IEC, Parte 1, Anexo SL. Los auditores deberían comprender que auditar un sistema de gestión es auditar los procesos de una organización y sus interacciones en relación con una o más normas de sistemas de gestión. Se logran resultados coherentes y predecibles de manera más eficaz y eficiente cuando las actividades se comprenden y se gestionan como procesos interrelacionados que funcionan como un sistema coherente.

A.2 Juicio profesional

Los auditores deberían aplicar su juicio profesional durante el proceso de auditoría y evitar concentrarse en los requisitos específicos de cada capítulo de la norma en detrimento de alcanzar el resultado previsto del sistema de gestión. Algunos capítulos de las normas de sistemas de gestión de ISO no se prestan fácilmente a la auditoría en términos de comparación entre un conjunto de criterios y el contenido de un procedimiento o una instrucción de trabajo. En estas situaciones, los auditores deberían usar su juicio profesional para determinar si la intención del capítulo se ha cumplido.

A.3 Resultados del desempeño

Los auditores deberían centrarse en el resultado previsto del sistema de gestión a lo largo del proceso de auditoría. Aunque son importantes los procesos y lo que deberían lograr, lo que cuenta es el resultado del sistema de gestión y su desempeño. También es importante considerar el nivel de integración de los diferentes sistemas de gestión y sus resultados previstos.

La ausencia de un proceso o de documentación puede ser importante en una organización de alto riesgo o compleja, pero no tan importante en otras organizaciones.

A.4 Verificación de la información

En la medida de lo posible, los auditores deberían considerar si la información proporciona evidencia objetiva suficiente para demostrar que se han cumplido los requisitos, como ser:

a) completa (todo el contenido esperado está en la información documentada);
b) correcta (el contenido es conforme con otras fuentes fiables, tales como normas y reglamentos);
c) coherente (la información documentada es coherente consigo misma y con documentos relacionados);
d) actual (el contenido está actualizado).

También debería tenerse en cuenta si la información que se está verificando proporciona evidencia objetiva suficiente para demostrar que se han cumplido los requisitos.

A.5 Muestreo

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

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

A.7 Auditoría del cumplimiento dentro de un sistema de gestión

El equipo auditor debería considerar si el auditado dispone de procesos eficaces para:

a) identificar sus requisitos legales y reglamentarios y otros requisitos con los que está comprometido;
b) gestionar sus actividades, productos y servicios para lograr el cumplimiento de estos requisitos;
c) evaluar su estado de cumplimiento.

Además de la orientación genérica proporcionada en este documento, al evaluar los procesos que el auditado ha implementado para asegurar el cumplimiento de los requisitos pertinentes, el equipo auditor debería tener en consideración si el auditado:

1) dispone de un proceso eficaz para identificar cambios en los requisitos de cumplimiento y para considerarlos como parte de la gestión del cambio;
2) dispone de personas competentes para gestionar sus procesos de cumplimiento;
3) mantiene y proporciona la información documentada apropiada sobre su estado de cumplimiento según lo requieran los organismos reglamentarios y otras partes interesadas;
4) incluye los requisitos de cumplimiento en su programa de auditoría interna;
5) trata todas las instancias de no cumplimiento;
6) tiene en consideración el desempeño del cumplimiento en sus revisiones por la dirección.

A.8 Auditoría del contexto

Muchas normas de sistemas de gestión requieren que una organización determine su contexto, incluyendo las necesidades y expectativas de las partes interesadas pertinentes y las cuestiones externas e internas. Para hacer esto, una organización puede usar varias técnicas de análisis y planificación estratégicas.

Los auditores deberían confirmar que se han desarrollado los procesos adecuados para esto, y que se usan eficazmente, de manera que sus resultados proporcionan una base fiable para determinar el alcance y el desarrollo del sistema de gestión. Para hacer esto, los auditores deberían tener en consideración la evidencia objetiva relativa a lo siguiente:

a) los procesos o métodos usados;
b) la idoneidad y la competencia de las personas que contribuyen a los procesos;
c) los resultados de los procesos;
d) la aplicación de los resultados para determinar el alcance y el desarrollo del sistema de gestión;
e) las revisiones periódicas del contexto, según sea apropiado.

A.9 Auditoría del liderazgo y el compromiso

Muchas normas de sistemas de gestión tienen requisitos adicionales para la alta dirección. Estos requisitos incluyen demostrar el compromiso y el liderazgo mediante la toma de responsabilidades sobre la eficacia del sistema de gestión y el cumplimiento de una serie de responsabilidades. Estas incluyen tareas que la alta dirección debería asumir por sí misma y otras que pueden delegarse.

Los auditores deberían obtener evidencia objetiva del grado en el que la alta dirección está implicada en la toma de decisiones relativas al sistema de gestión y la manera en que demuestra el compromiso para asegurar su eficacia. Esto puede lograrse revisando los resultados de los procesos pertinentes (por ejemplo las políticas, los objetivos, los recursos disponibles, las comunicaciones de la alta dirección) y entrevistando al personal para determinar el grado de compromiso de la alta dirección.

Los auditores también deberían intentar entrevistar a la alta dirección para confirmar que tienen una comprensión adecuada de las cuestiones específicas de la disciplina pertinentes para su sistema de gestión, junto con el contexto en el que opera su organización, de manera que puedan asegurar que el sistema de gestión alcanza sus resultados previstos.

Los auditores no deberían centrarse en el liderazgo sólo al nivel de la alta dirección, sino que deberían auditar el liderazgo y el compromiso a otros niveles de dirección, según sea apropiado.

A.10 Auditoría de riesgos y oportunidades

La determinación y la gestión de los riesgos y oportunidades de la organización pueden incluirse como parte de la asignación de una auditoría individual. Los objetivos principales para una asignación de una auditoría de este tipo son:

- asegurar la credibilidad de los procesos de identificación de riesgos y oportunidades;
- asegurarse de que los riesgos y oportunidades se determinan y gestionan correctamente;
- revisar la manera en que la organización aborda los riesgos y oportunidades que ha determinado.

Una auditoría del enfoque de una organización a la determinación de riesgos y oportunidades no debería desempeñarse como una actividad aislada. Debería estar implícita durante toda la auditoría de un sistema de gestión, incluso durante la entrevista con la alta dirección. Un auditor debería actuar de acuerdo con los siguientes pasos y recopilar evidencias objetivas de la siguiente manera:

a) entradas usadas por la organización para determinar sus riesgos y oportunidades, que pueden incluir:
   - el análisis de las cuestiones externas e internas;
   - la dirección estratégica de la organización;
   - las partes interesadas relacionadas con su sistema de gestión de la disciplina específica, así como sus requisitos,
   - las fuentes potenciales de riesgos como los aspectos ambientales y los peligros para la seguridad, etc.
b) método por el que se evalúan los riesgos y oportunidades, que puede diferir entre disciplinas y sectores.

El tratamiento que la organización hace de sus riesgos y oportunidades, incluyendo el nivel de riesgo que desea aceptar y la manera en que lo controla, requerirá la aplicación de juicio profesional por parte del auditor.

A.11 Ciclo de vida

Algunos sistemas de gestión específicos de una disciplina requieren la aplicación de una perspectiva de ciclo de vida a sus productos y servicios. Los auditores no deberían considerar esto como un requisito para adoptar un enfoque de ciclo de vida. Una perspectiva de ciclo de vida implica considerar el control y la influencia que la organización tiene sobre las etapas del ciclo de vida de sus productos y servicios. Las etapas en un ciclo de vida incluyen la adquisición de materias primas, el diseño, producción, transporte/entrega, uso, tratamiento al final de la vida útil, y disposición final. Este enfoque permite a la organización identificar aquellas áreas en las que, al considerar su alcance, puede minimizar su impacto en el medio ambiente al tiempo que añade valor a la organización. El auditor debería usar su juicio profesional sobre la manera en que la organización ha aplicado la perspectiva de ciclo de vida en términos de su estrategia y de:

a) la vida del producto o servicio;
b) la influencia de la organización sobre la cadena de suministro;
c) la longitud de la cadena de suministro;
d) la complejidad tecnológica del producto.

Cuando una organización ha combinado varios sistemas de gestión en un único sistema de gestión para cumplir sus propias necesidades, el auditor debería observar cuidadosamente cualquier superposición concerniente a la consideración del ciclo de vida.

A.12 Auditoría de la cadena de suministro

Puede requerirse la auditoría de la cadena de suministro para requisitos específicos. El programa de auditoría del proveedor debería desarrollarse con los criterios de auditoría aplicables para el tipo de suministradores y proveedores externos. El alcance de la auditoría de la cadena de suministro puede diferir, por ejemplo, auditoría del sistema de gestión completo, auditoría de un único proceso, auditoría de un producto, auditoría de la configuración.

A.13 Preparación de los documentos de trabajo de auditoría

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

a) ¿Qué registro de auditoría se creará utilizando este documento de trabajo?
b) ¿Con qué actividad de la auditoría está relacionado este documento de trabajo en particular?
c) ¿Quién será el usuario de este documento de trabajo?
d) ¿Qué información se necesita para preparar este documento de trabajo?

A.14 Selección de las fuentes de información

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

a) entrevistas con empleados y con otras personas;
b) observación de actividades y el ambiente de trabajo y condiciones circundantes;
c) información documentada, como políticas, objetivos, planes, procedimientos, normas, instrucciones, licencias y permisos, especificaciones, planos, contratos y pedidos;
d) registros, tales como registros de inspección, actas de reuniones, informes de auditoría, registros de programas de seguimiento y resultados de mediciones;
e) resúmenes de datos, análisis e indicadores de desempeño;
f) información sobre los planes de muestreo del auditado y sobre cualquier procedimiento para el control de los procesos de muestreo y medición;
g) informes de otras fuentes, por ejemplo, retroalimentación del cliente, encuestas y mediciones externas, otra información pertinente de partes externas y la calificación de los proveedores externos;
h) bases de datos y sitios web;
i) simulaciones y modelizaciones.

A.15 Visita a la ubicación del auditado

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

a) Planificar la visita:
- asegurar la autorización y el acceso a aquellas partes de la ubicación del auditado, para visitarlas de acuerdo con el alcance de la auditoría;
- proporcionar la información adecuada a los auditores sobre seguridad física, salud (por ejemplo, cuarentena), cuestiones de seguridad y salud en el trabajo y normas culturales y horas de trabajo para la visita, incluyendo la vacunación y autorizaciones requeridas y recomendadas, si es aplicable;
- confirmar con el auditado que cualquier equipo de protección personal (EPP) estará disponible para el equipo auditor, si es aplicable;
- confirmar los acuerdos con el auditado sobre el uso de dispositivos móviles y cámaras, incluyendo la grabación de información como fotografías de ubicaciones y equipos, copias de capturas de pantalla o fotocopias de documentos, vídeos de actividades y entrevistas, teniendo en cuenta las cuestiones de seguridad y confidencialidad;
- excepto para auditorías *ad hoc* no programadas, asegurarse de que el personal visitado será informado sobre los objetivos y el alcance de la auditoría.

b) Actividades *in situ*:
- evitar cualquier interrupción innecesaria de los procesos operativos;
- asegurarse de que el equipo auditor está utilizando el EPP correctamente (si procede);
- asegurarse de que se comunican los procedimientos de emergencia (por ejemplo, salidas de emergencia, puntos de reunión);
- programar la comunicación para minimizar las interrupciones;
- adaptar el tamaño del equipo auditor y el número de guías y observadores de acuerdo con el alcance de la auditoría, para evitar interferencias con los procesos operativos tanto como sea posible;
- no tocar ni manipular ningún equipo, a menos que se permita explícitamente, incluso cuando se tenga la competencia o se esté autorizado;
- si tiene lugar un incidente durante la visita *in situ*, el líder del equipo auditor debería revisar la situación con el auditado y, si es necesario, con el cliente de la auditoría y llegar a un acuerdo sobre si la auditoría se debería interrumpir, volver a programar o continuar;
- si se hacen copias de documentos en cualquier medio, pedir permiso con antelación y considerar las cuestiones de confidencialidad y seguridad;
- cuando se toman notas, evitar recopilar información personal a menos que lo requieran los objetivos de la auditoría o los criterios de auditoría.

c) Actividades de la auditoría virtual:
- asegurarse de que el equipo auditor está usando los protocolos de acceso remoto acordados, incluyendo los dispositivos, software, etc. requeridos;
- si se toman copias de capturas de pantalla de documentos de cualquier tipo, pedir permiso por adelantado y considerar las cuestiones de confidencialidad y seguridad, y evitar grabar a las personas sin su permiso;
- si sucede un incidente durante el acceso remoto, el líder del equipo auditor debería revisar la situación con el auditado y, si es necesario, con el cliente de la auditoría, y llegar a un acuerdo sobre si la auditoría se debería interrumpir, reprogramar o

continuar;
- usar planos/diagramas de planta de la ubicación remota como referencia;
- mantener el respeto a la privacidad durante las pausas en la auditoría.

Es necesario tener en cuenta la disposición de la información y de las evidencias de auditoría, independientemente del tipo de medio, más adelante, una vez que haya pasado la necesidad de su conservación.

A.16 Auditoría de actividades y ubicaciones virtuales

Las auditorías virtuales se realizan cuando una organización desempeña trabajo o proporciona un servicio usando un entorno en línea que permite a las personas con independencia de la ubicación física, ejecutar procesos (por ejemplo, la intranet de la empresa, una "computación en la nube"). A veces se refiere a la auditoría de una ubicación virtual como auditoría virtual. Las auditorías remotas hacen referencia al uso de tecnología para recopilar información, entrevistar a un auditado, etc., cuando los métodos "cara a cara" no son posibles o deseables.

Una auditoría virtual sigue el proceso estándar de auditoría a la vez que se usa la tecnología para verificar las evidencias objetivas. El auditado y el equipo auditor deberían asegurar los requisitos tecnológicos apropiados para las auditorías virtuales, que pueden incluir:

- asegurarse de que el equipo auditor está usando los protocolos de acceso remoto acordados, incluyendo los dispositivos, software, etc. requeridos;
- realizar verificaciones técnicas antes de la auditoría para resolver cuestiones técnicas;
- asegurarse de que se dispone de planes de contingencia y de que se comunican (por ejemplo, interrupción del acceso, uso de tecnologías alternativas), incluyendo la provisión de tiempo adicional para la auditoría si es necesario.

La competencia del auditor debería incluir:

- habilidades técnicas para usar los equipos electrónicos apropiados y otras tecnologías durante la auditoría;
- experiencia en facilitar reuniones virtualmente para realizar la auditoría de manera remota.

Al llevar a cabo la reunión de apertura o la auditoría virtual, el auditor debería tener en consideración los siguientes elementos:

- los riesgos asociados con las auditorías virtuales o remotas;
- usar planos/diagramas de planta de las ubicaciones remotas como referencia o para asignar información electrónica;
- facilitar la prevención de interferencias e interrupciones en la señal por ruidos de fondo;
- pedir permiso por adelantado para tomar capturas de pantalla de documentos o cualquier tipo de grabación, y considerar las cuestiones de confidencialidad y seguridad;
- asegurar la confidencialidad y la privacidad durante las pausas en la auditoría, por

ejemplo silenciando los micrófonos, pausando las cámaras.

A.17 Realización de entrevistas

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

a) las entrevistas deberían mantenerse con personas de los niveles y funciones apropiados que desempeñan actividades o tareas dentro del alcance de la auditoría;
b) las entrevistas normalmente deberían llevarse a cabo durante la jornada de trabajo normal y, cuando sea posible, en el lugar de trabajo normal de la persona entrevistada;
c) debería intentarse que la persona entrevistada esté cómoda antes de la entrevista y durante la misma;
d) debería explicarse la razón de la entrevista y cualquier toma de notas;
e) las entrevistas pueden iniciarse solicitando a las personas que describan su trabajo;
f) debería seleccionarse cuidadosamente el tipo de preguntas utilizado (por ejemplo, preguntas abiertas, cerradas, inductivas, indagaciones apreciativas);
g) tomar conciencia de la limitación en la comunicación no verbal en los entornos virtuales; en su lugar, debería hacerse hincapié en el tipo de preguntas a usar para encontrar evidencias objetivas;
h) los resultados de la entrevista deberían resumirse y revisarse con la persona entrevistada;
i) debería agradecerse a las personas entrevistadas su participación y cooperación.

A.18 Hallazgos de la auditoría

A.18.1 Determinación de los hallazgos de la auditoría

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

a) el seguimiento de los registros y las conclusiones de auditorías previas;
b) los requisitos del cliente de la auditoría;
c) la exactitud, la suficiencia y la adecuación de las evidencias objetivas para apoyar los hallazgos de la auditoría;
d) el grado en que se han realizado las actividades de auditoría planificadas y en que se han logrado los resultados planificados;
e) los hallazgos que excedan la práctica normal, o las oportunidades de mejora;
f) el tamaño de muestra;
g) la categorización (si existe) de los hallazgos de la auditoría.

A.18.2 Registro de conformidades

Para los registros de conformidad, debería considerarse lo siguiente:

a) la descripción de o la referencia a los criterios de auditoría respecto a los cuales se

muestra la conformidad;
b) la evidencia de la auditoría para respaldar la conformidad y la eficacia, si es aplicable;
c) la declaración de conformidad, si es aplicable.

A.18.3 Registro de no conformidades

Para los registros de no conformidad, debería considerarse lo siguiente:

a) la descripción de los criterios de auditoría o la referencia a los mismos;
b) la evidencia de la auditoría;
c) la declaración de no conformidad;
d) los hallazgos de la auditoría relacionados, si es aplicable.

A.18.4 Tratamiento de los hallazgos relacionados con múltiples criterios

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

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

a) hallazgos separados para cada criterio; o
b) un único hallazgo, combinando las referencias a los múltiples criterios.

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