certiprof®

ISO/IEC 42001

INTERNAL AUDITOR

PROFESSIONAL CERTIFICATION

I42001IA™ Versión 012026

Introducción

Contenido

La inteligencia artificial (IA) se aplica cada vez más en todos los sectores que utilizan tecnologías de la información y se espera que sea uno de los principales impulsores económicos.

Una consecuencia de esta tendencia es que determinadas aplicaciones pueden dar lugar a desafíos sociales en los próximos años.

Este documento tiene como objetivo ayudar a las organizaciones a desempeñar responsablemente su papel con respecto a los sistemas de IA (p. ej., usar, desarrollar, monitorear o proporcionar productos o servicios que utilicen IA).

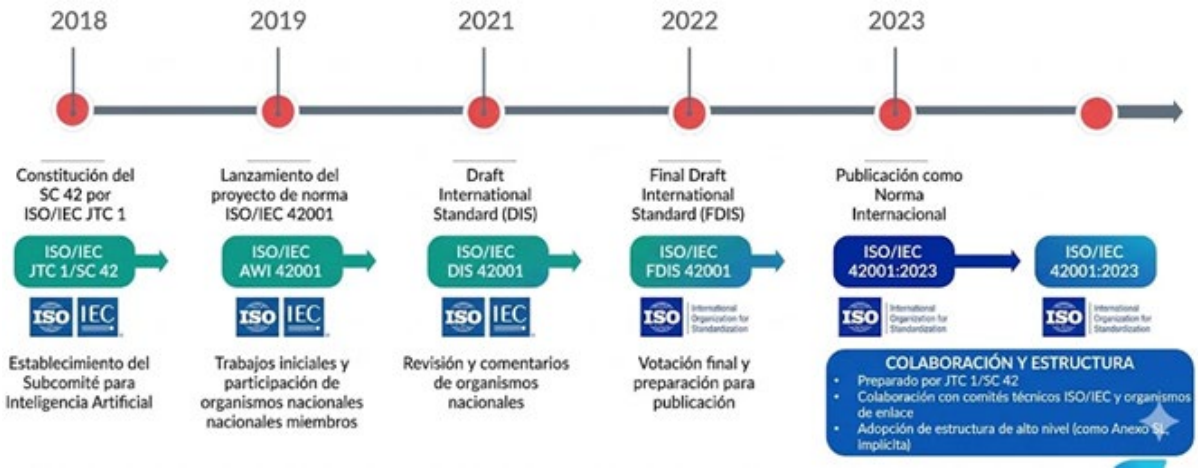
Sistema de Gestión de Inteligencia Artificial (SGIA)

Este documento proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de inteligencia artificial dentro del contexto de una organización.

Se espera que las organizaciones centren su aplicación de los requisitos en características que son únicas de la IA.

Ciertas características de la IA, como la capacidad de aprender y mejorar continuamente o la falta de transparencia o explicabilidad, pueden justificar salvaguardas diferentes si plantean preocupaciones adicionales en comparación con cómo se realizaría tradicionalmente la tarea.

Historia de la Norma



Este documento fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnologías de la información, Subcomité SC 42, Inteligencia artificial.

Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para abordar campos particulares de actividad técnica.

NOTA

Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en enlace con ISO e IEC, también participan en el trabajo.

ISO/IEC 42001:2023 — Estructura

Prólogo
Introducción

1 Alcance
2 Referencias normativas
3 Términos y definiciones
4 Contexto de la organización
5 Liderazgo
6 Planificación
7 Soporte
8 Operación
9 Evaluación del desempeño
10 Mejora

Ciclo Deming PHVA y SGIA

La adopción de un sistema de gestión de IA para extender las estructuras de gestión existentes es una decisión estratégica para una organización.

Las necesidades y objetivos de la organización, los procesos, el tamaño y la estructura, así como las expectativas de diversas partes interesadas, influyen en el establecimiento e implementación del sistema de gestión de IA.

Las organizaciones pueden optar por aplicar estos requisitos utilizando un enfoque basado en riesgos para garantizar que se aplique el nivel adecuado de control para los casos de uso, servicios o productos de IA dentro del alcance de la organización.

NOTA
Este documento aplica la estructura armonizada (números de cláusula idénticos, títulos de cláusula, texto y términos comunes y definiciones núcleo) desarrollada para mejorar la alineación entre las normas de sistemas de gestión (MSS).

ISO 42001: Familia de Normas

Contenido
Los siguientes documentos se citan en el texto de tal forma que parte o la totalidad de su contenido constituye requisitos de este documento. Para referencias fechadas, solo aplica la edición citada. Para referencias no fechadas, aplica la edición más reciente del documento referenciado (incluidas sus enmiendas).

ISO/IEC 22989:2022, Tecnología de la información — Inteligencia artificial — Conceptos y terminología de inteligencia artificial.

Alcance, Referencias Normativas y Términos

Cláusula 1: Alcance

Este documento especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de inteligencia artificial dentro del contexto de una organización.

Este documento está destinado a ser utilizado por una organización que proporcione o utilice productos o servicios que utilicen sistemas de inteligencia artificial.

Este documento tiene como objetivo ayudar a la organización a desarrollar, proporcionar o utilizar sistemas de IA de manera responsable mientras persigue sus objetivos y cumple los requisitos aplicables, las obligaciones relacionadas con las partes interesadas y las expectativas de estas.

Este documento es aplicable a cualquier organización, independientemente de su tamaño, tipo o naturaleza, que proporcione o utilice productos o servicios que utilicen sistemas de inteligencia artificial.

Cláusula 2: Referencias Normativas

Los siguientes documentos se citan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos de este documento.

Para las referencias fechadas, solo se aplica la edición citada.

Para las referencias no fechadas, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO/IEC 22989:2022
Tecnología de la información — Inteligencia artificial — Conceptos y terminología de inteligencia artificial.

Cláusula 3: Términos y definiciones

Para los propósitos de este documento, se aplican los términos y definiciones dados en **ISO/IEC 22989** y los siguientes.

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

— Plataforma de navegación en línea de ISO: https://www.iso.org/obp
— IEC Electropedia: https://www.electropedia.org/

Organización (3.1)

Contenido

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

NOTA 1
El concepto de organización incluye, entre otros, comerciante individual, empresa, corporación, firma, autoridad, asociación, organización benéfica o institución, o parte o combinación de estas, ya sea incorporada o no, pública o privada.

NOTA 2
Si la organización es parte de una entidad más grande, el término "organización" se refiere únicamente a la parte de la entidad mayor que está dentro del alcance del sistema de gestión de IA.

Parte interesada (3.2)

Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o actividad.

NOTA

Una visión general de las partes interesadas en inteligencia artificial se proporciona en **ISO/IEC 22989:2022**.

Alta dirección (3.3)

Persona o grupo de personas que dirige y controla una organización al más alto nivel.

NOTA

La alta dirección tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización.

Sistema de gestión (3.4)

Conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas y objetivos, así como procesos para lograr dichos objetivos.

Política (3.5)

Intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

Objetivo (3.6)

Resultado a lograr.

NOTA

Un objetivo puede ser estratégico, táctico u operativo.

Riesgo (3.7)

Efecto de la incertidumbre sobre los objetivos.

NOTA

Un efecto es una desviación de lo esperado, ya sea positiva o negativa.

Proceso (3.8)

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

Competencia (3.9)

Contenido

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

Información documentada (3.10)

Información que una organización debe controlar y mantener, y el medio que la contiene.

NOTA

La información documentada puede estar en cualquier formato o medio y provenir de cualquier fuente.

Desempeño (3.11)

Resultado medible.

NOTA

El desempeño puede relacionarse con hallazgos cuantitativos o cualitativos.

Mejora continua (3.12)

Actividad recurrente para mejorar el desempeño.

Auditoría (3.13)

Proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla de manera objetiva para determinar el grado en que se cumplen los criterios de auditoría.

Cláusula 4 — Contexto de la organización

4.1 Comprensión de la organización y su contexto

La organización debe determinar las cuestiones externas e internas que son relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de inteligencia artificial.

La organización debe determinar si el cambio climático es una cuestión relevante.

La organización debe considerar el propósito previsto de los sistemas de IA que desarrolla, proporciona o utiliza.

La organización debe determinar sus roles con respecto a los sistemas de IA.

NOTA 1

Para comprender la organización y su contexto, puede ser útil determinar el rol o roles de la organización con respecto al sistema de IA.

Estos roles pueden incluir:

— proveedor de IA
— productor de IA
— cliente de IA
— socio de IA
— sujeto de IA
— autoridad de IA

Un rol puede aplicarse a toda la organización o solo a una parte de la organización.

Una organización puede tener más de un rol.

Las orientaciones sobre los roles de las partes interesadas se proporcionan en **ISO/IEC 22989**.

El **NIST AI Risk Management Framework** también proporciona información sobre roles relacionados con sistemas de IA.

NOTA 2

Las cuestiones externas e internas pueden incluir, entre otras:

a) contexto externo, como:

1. requisitos legales y regulatorios
2. incentivos
3. factores sociales, culturales y éticos
4. panorama competitivo
5. cambios en el entorno tecnológico

b) contexto interno, como:

1. valores, cultura y ética organizacional
2. políticas y estrategias organizacionales
3. capacidades y recursos de la organización.

NOTA 3

Si la organización trata información de identificación personal (PII), los roles de controlador y procesador de PII pueden ser relevantes.

Las orientaciones sobre estos roles se proporcionan en **ISO/IEC 29100**.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

— las partes interesadas que son relevantes para el sistema de gestión de IA;

— los requisitos relevantes de estas partes interesadas;

— cuáles de estos requisitos se abordarán a través del sistema de gestión de IA.

NOTA

Las partes interesadas relevantes pueden tener requisitos relacionados con el cambio climático.

4.3 Determinación del alcance del sistema de gestión de inteligencia artificial

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de IA para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

— las cuestiones externas e internas mencionadas en 4.1;

— los requisitos mencionados en 4.2.

El alcance debe estar disponible como información documentada.

El alcance del sistema de gestión de IA debe determinar las actividades de la organización con respecto a los requisitos de este documento relacionados con:

— el sistema de gestión de IA
— liderazgo
— planificación
— soporte

— operación
— evaluación del desempeño
— mejora
— controles
— objetivos.

4.4 Sistema de gestión de inteligencia artificial

La organización debe establecer, implementar, mantener, mejorar continuamente y documentar un sistema de gestión de inteligencia artificial, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

5 Liderazgo

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de inteligencia artificial mediante:

— asegurar que la política de IA (véase 5.2) y los objetivos de IA (véase 6.2) se establezcan y sean compatibles con la dirección estratégica de la organización;

— asegurar la integración de los requisitos del sistema de gestión de IA en los procesos de negocio de la organización;

— asegurar que los recursos necesarios para el sistema de gestión de IA estén disponibles;

— comunicar la importancia de una gestión eficaz de la IA y del cumplimiento de los requisitos del sistema de gestión de IA;

— asegurar que el sistema de gestión de IA logre sus resultados previstos;

— dirigir y apoyar a las personas para contribuir a la eficacia del sistema de gestión de IA;

— promover la mejora continua;

— apoyar a otros roles relevantes para demostrar su liderazgo en lo que respecta a sus áreas de responsabilidad.

NOTA 1

La referencia a "negocio" en este documento puede interpretarse de manera amplia para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

NOTA 2

Establecer, fomentar y modelar una cultura dentro de la organización para adoptar un enfoque responsable en el uso, desarrollo y gobernanza de los sistemas de IA puede ser una demostración importante del compromiso y liderazgo de la alta dirección. Garantizar la concienciación y el cumplimiento de dicho enfoque responsable en apoyo del sistema de gestión de IA mediante el liderazgo puede contribuir al éxito del sistema de gestión de IA.

5.2 Política de IA

La alta dirección debe establecer una política de inteligencia artificial que:

a) sea apropiada al propósito de la organización;

b) proporcione un marco para establecer los objetivos de IA (véase 6.2);

c) incluya un compromiso de cumplir con los requisitos aplicables;

d) incluya un compromiso de mejora continua del sistema de gestión de IA.

5.2 Política de IA

La política de IA debe:

— estar disponible como información documentada;

— hacer referencia, cuando sea relevante, a otras políticas organizacionales;

— ser comunicada dentro de la organización;

— estar disponible para las partes interesadas, según corresponda.

Los objetivos de control y controles para establecer una política de IA se proporcionan en **A.2 en la Tabla A.1**.

La orientación de implementación para estos controles se proporciona en **B.2**.

NOTA

Las consideraciones para las organizaciones al desarrollar políticas de IA se proporcionan en **ISO/IEC 38507**.

5.3 Roles, responsabilidades y autoridades

La alta dirección debe asegurar que las responsabilidades y autoridades para los roles relevantes se asignen y comuniquen dentro de la organización.

5.3 Roles, responsabilidades y autoridades

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurar que el sistema de gestión de IA cumpla con los requisitos de este documento;

b) informar sobre el desempeño del sistema de gestión de IA a la alta dirección.

NOTA

Se proporciona un control para definir y asignar roles y responsabilidades en **A.3.2 en la Tabla A.1**.

La orientación de implementación para este control se proporciona en **B.3.2**.

6 Planificación

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 General

Al planificar el sistema de gestión de inteligencia artificial, la organización debe considerar las cuestiones mencionadas en **4.1** y los requisitos mencionados en **4.2** y determinar los riesgos y oportunidades que deben abordarse para:

— dar garantía de que el sistema de gestión de IA puede lograr sus resultados previstos;

— prevenir o reducir efectos no deseados;

— lograr la mejora continua.

6.1.1 General

Contenido

La organización debe establecer y mantener criterios de riesgo de IA que apoyen:

— distinguir los riesgos aceptables de los no aceptables;

— realizar evaluaciones de riesgo de IA;

— llevar a cabo el tratamiento de riesgos de IA;

— evaluar los impactos de riesgos de IA.

NOTA 1

Las consideraciones para determinar la cantidad y tipo de riesgo que una organización está dispuesta a perseguir o retener se proporcionan en **ISO/IEC 38507** e **ISO/IEC 23894**.

6.1.1 General

Contenido

La organización debe determinar los riesgos y oportunidades de acuerdo con:

— el dominio y el contexto de aplicación de un sistema de IA;

— el uso previsto;

— el contexto externo e interno descrito en **4.1**.

NOTA 2

Más de un sistema de IA puede ser considerado dentro del alcance del sistema de gestión de IA. En este caso, la determinación de oportunidades y usos se realiza para cada sistema de IA o agrupaciones de sistemas de IA.

6.1.1 General

La organización debe planificar:

a) acciones para abordar estos riesgos y oportunidades;

b) cómo:

1. integrar e implementar las acciones en sus procesos del sistema de gestión de IA;

2. evaluar la eficacia de estas acciones.

6.1.1 General

La organización debe conservar información documentada sobre las acciones tomadas para identificar y abordar riesgos de IA y oportunidades de IA.

NOTA 3

Se proporciona orientación sobre cómo implementar la gestión de riesgos para organizaciones que desarrollan, proporcionan o utilizan productos, sistemas y servicios de IA en **ISO/IEC 23894**.

NOTA 4

El contexto de la organización y sus actividades puede tener un impacto en las actividades de gestión de riesgos de la organización.

6.1.1 General

NOTA 5

La forma de definir el riesgo y, por lo tanto, de concebir la gestión de riesgos puede variar entre sectores e industrias.

La definición de riesgo en **3.7** permite una visión amplia del riesgo adaptable a cualquier sector, como los sectores mencionados en **Anexo D**.

En cualquier caso, es responsabilidad de la organización, como parte de la evaluación de riesgos, adoptar primero una visión de riesgo adaptada a su contexto.

Esto puede incluir abordar el riesgo mediante definiciones utilizadas en sectores donde el sistema de IA se desarrolla y utiliza, como la definición de **ISO/IEC Guide 51**.

6.1.2 Evaluación de riesgos de IA

La organización debe definir y establecer un proceso de evaluación de riesgos de IA que:

a) esté informado y alineado con la política de IA (véase **5.2**) y los objetivos de IA (véase **6.2**);

6.1.2 Evaluación de riesgos de IA

b) esté diseñado de tal manera que evaluaciones repetidas de riesgos de IA puedan producir resultados consistentes, válidos y comparables;

c) identifique riesgos que ayuden o impidan lograr sus objetivos de IA;

6.1.2 Evaluación de riesgos de IA

d) analice los riesgos de IA para:

1. evaluar las posibles consecuencias para la organización, los individuos y las sociedades que resultarían si los riesgos identificados se materializan;

2. evaluar, cuando sea aplicable, la probabilidad realista de los riesgos identificados;

3. determinar los niveles de riesgo.

6.1.2 Evaluación de riesgos de IA

e) evalúe los riesgos de IA para:

1. comparar los resultados del análisis de riesgos con los criterios de riesgo (véase **6.1.1**);

2. priorizar los riesgos evaluados para el tratamiento de riesgos.

6.1.2 Evaluación de riesgos de IA

La organización debe conservar información documentada sobre el proceso de evaluación de riesgos de IA.

NOTA

Al evaluar las consecuencias como parte de **6.1.2 d) 1)**, la organización puede utilizar una evaluación de impacto del sistema de IA como se indica en **6.1.4**.

6.1.3 Tratamiento de riesgos de IA

Teniendo en cuenta los resultados de la evaluación de riesgos, la organización debe definir un proceso de tratamiento de riesgos de IA para:

a) seleccionar opciones apropiadas de tratamiento de riesgos de IA;

6.1.3 Tratamiento de riesgos de IA

b) determinar todos los controles necesarios para implementar las opciones de tratamiento de riesgos de IA elegidas y comparar los controles con los del **Anexo A** para verificar que no se haya omitido ningún control necesario;

NOTA 1

El **Anexo A** proporciona controles de referencia para cumplir objetivos organizacionales y abordar riesgos relacionados con el diseño y uso de sistemas de IA.

6.1.3 Tratamiento de riesgos de IA

c) considerar los controles del **Anexo A** que sean relevantes para la implementación de las opciones de tratamiento de riesgos de IA;

d) identificar si son necesarios controles adicionales más allá de los del **Anexo A** para implementar todas las opciones de tratamiento de riesgos.

6.1.3 Tratamiento de riesgos de IA

e) considerar la orientación del **Anexo B** para la implementación de los controles determinados en **b)** y **c)**.

NOTA 2

Los objetivos de control están implícitamente incluidos en los controles elegidos.

La organización puede seleccionar un conjunto apropiado de objetivos de control y controles del **Anexo A**.

Los controles del **Anexo A** no son exhaustivos y pueden ser necesarios objetivos y controles adicionales.

6.1.3 Tratamiento de riesgos de IA

f) producir una **declaración de aplicabilidad** que contenga los controles necesarios y proporcionar justificación para la inclusión y exclusión de controles.

NOTA 3

La organización puede proporcionar justificaciones documentadas para excluir cualquier objetivo de control en general o para sistemas de IA específicos.

6.1.3 Tratamiento de riesgos de IA

g) formular un plan de tratamiento de riesgos de IA.

La organización debe obtener aprobación de la dirección designada para el plan de tratamiento de riesgos de IA y para la aceptación de los riesgos residuales de IA.

6.1.3 Tratamiento de riesgos de IA

Los controles necesarios deben ser:

— alineados con los objetivos en **6.2**;

— disponibles como información documentada;

— comunicados dentro de la organización;

— disponibles para las partes interesadas, según corresponda.

6.1.3 Tratamiento de riesgos de IA

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de IA.

6.1.4 Evaluación de impacto del sistema de IA

La organización debe definir un proceso para evaluar las posibles consecuencias para individuos o grupos de individuos, o ambos, y las sociedades que pueden resultar del desarrollo, provisión o uso de sistemas de IA.

6.1.4 Evaluación de impacto del sistema de IA

La evaluación de impacto del sistema de IA debe determinar las posibles consecuencias que el despliegue, el uso previsto y el uso indebido previsible de un sistema de IA tiene sobre individuos o grupos de individuos, o ambos, y las sociedades.

6.1.4 Evaluación de impacto del sistema de IA

La evaluación de impacto del sistema de IA debe tener en cuenta el contexto técnico y social específico donde se despliega el sistema de IA y las jurisdicciones aplicables.

6.1.4 Evaluación de impacto del sistema de IA

El resultado de la evaluación de impacto del sistema de IA debe documentarse.

Cuando sea apropiado, el resultado de la evaluación de impacto del sistema puede ponerse a disposición de las partes interesadas relevantes definidas por la organización.

6.1.4 Evaluación de impacto del sistema de IA

La organización debe considerar los resultados de la evaluación de impacto del sistema de IA en la evaluación de riesgos (véase **6.1.2**).

Los controles para evaluar impactos de sistemas de IA se proporcionan en **A.5 en la Tabla A.1**.

NOTA

En algunos contextos (como sistemas de IA críticos para seguridad o privacidad), la organización puede requerir evaluaciones de impacto específicas de disciplina como parte de las actividades generales de gestión de riesgos.

6.2 Objetivos de IA y planificación para lograrlos

La organización debe establecer objetivos de IA en funciones y niveles relevantes.

6.2 Objetivos de IA y planificación para lograrlos

Los objetivos de IA deben:

a) ser coherentes con la política de IA (véase **5.2**);

b) ser medibles (si es practicable);

c) tener en cuenta los requisitos aplicables;

d) ser monitoreados;

6.2 Objetivos de IA y planificación para lograrlos

e) ser comunicados;

f) actualizarse según corresponda;

g) estar disponibles como información documentada.

6.2 Objetivos de IA y planificación para lograrlos

Al planificar cómo lograr sus objetivos de IA, la organización debe determinar:

— qué se hará;

— qué recursos se requerirán;

— quién será responsable;

— cuándo se completará;

— cómo se evaluarán los resultados.

6.2 Objetivos de IA y planificación para lograrlos

NOTA

Se proporciona una lista no exhaustiva de objetivos de IA relacionados con la gestión de riesgos en el **Anexo C**.

Los objetivos de control y controles para identificar objetivos para el desarrollo y uso responsable de sistemas de IA y las medidas para lograrlos se proporcionan en **A.6.1** y **A.9.3 en la Tabla A.1**.

La orientación de implementación para estos controles se proporciona en **B.6.1** y **B.9.3**.

6.3 Planificación de cambios

Cuando la organización determine la necesidad de cambios en el sistema de gestión de IA, los cambios deben llevarse a cabo de manera planificada.

---

7 Soporte

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de IA.

NOTA

Los objetivos de control y controles para recursos de IA se proporcionan en **A.4 en la Tabla A.1**.

La orientación de implementación para estos controles se proporciona en **Cláusula B.4**.

7.2 Competencia

La organización debe:

— determinar la competencia necesaria de las personas que realizan trabajos bajo su control que afectan su desempeño en IA;

7.2 Competencia

— asegurar que estas personas sean competentes con base en educación, formación o experiencia apropiada;

— cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.

7.2 Competencia

La información documentada apropiada debe estar disponible como evidencia de la competencia.

7.2 Competencia

NOTA 1

La orientación de implementación para recursos humanos, incluyendo la consideración de la experiencia necesaria, se proporciona en **B.4.6**.

NOTA 2

Las acciones aplicables pueden incluir, por ejemplo: la provisión de formación a, la mentoría de, o la reasignación de personas actualmente empleadas; o la contratación o subcontratación de personas competentes.

7.3 Concienciación

Las personas que realizan trabajos bajo el control de la organización deben ser conscientes de:

— la política de IA (véase **5.2**);

7.3 Concienciación

— su contribución a la eficacia del sistema de gestión de IA, incluidos los beneficios de mejorar el desempeño de la IA;

— las implicaciones de no cumplir con los requisitos del sistema de gestión de IA.

7.4 Comunicación

La organización debe determinar las comunicaciones internas y externas relevantes para el sistema de gestión de IA, incluyendo:

— qué comunicará;

— cuándo comunicar;

7.4 Comunicación

— con quién comunicar;

— cómo comunicar.

7.5 Información documentada

7.5.1 General

El sistema de gestión de IA de la organización debe incluir:

a) información documentada requerida por este documento;

b) información documentada determinada por la organización como necesaria para la eficacia del sistema de gestión de IA.

7.5.1 General

NOTA

La extensión de la información documentada para un sistema de gestión de IA puede diferir de una organización a otra debido a:

— el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

— la complejidad de los procesos y sus interacciones;

— la competencia de las personas.

7.5.2 Creación y actualización de información documentada

Al crear y actualizar información documentada, la organización debe asegurar la apropiada:

— identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

7.5.2 Creación y actualización de información documentada

— formato (por ejemplo, idioma, versión del software, gráficos) y medio (por ejemplo, papel, electrónico);

— revisión y aprobación para idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de IA y por este documento debe ser controlada para asegurar:

a) que esté disponible y sea adecuada para su uso, donde y cuando se necesite;

b) que esté adecuadamente protegida (por ejemplo, contra pérdida de confidencialidad, uso indebido o pérdida de integridad).

7.5.3 Control de la información documentada

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

— distribución, acceso, recuperación y uso;

— almacenamiento y preservación, incluyendo la preservación de la legibilidad;

7.5.3 Control de la información documentada

— control de cambios (por ejemplo, control de versiones);

— retención y disposición.

7.5.3 Control de la información documentada

La información documentada de origen externo determinada por la organización como necesaria para la planificación y operación del sistema de gestión de IA debe ser identificada, según corresponda, y controlada.

NOTA

El acceso puede implicar una decisión respecto al permiso para ver únicamente la información documentada o al permiso y autoridad para ver y cambiar la información documentada.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en **Cláusula 6**, mediante:

— el establecimiento de criterios para los procesos;

— la implementación del control de los procesos de acuerdo con los criterios.

8.1 Planificación y control operacional

La organización debe implementar los controles determinados de acuerdo con **6.1.3** que estén relacionados con la operación del sistema de gestión de IA (por ejemplo, controles relacionados con el ciclo de vida de desarrollo y uso del sistema de IA).

8.1 Planificación y control operacional

La eficacia de estos controles debe ser monitoreada y deben considerarse acciones correctivas si no se logran los resultados previstos.

El **Anexo A** enumera controles de referencia y el **Anexo B** proporciona orientación de implementación para ellos.

8.1 Planificación y control operacional

La información documentada debe estar disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

8.1 Planificación y control operacional

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no intencionados, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

8.1 Planificación y control operacional

La organización debe asegurar que los procesos, productos o servicios proporcionados externamente que sean relevantes para el sistema de gestión de IA sean controlados.

8.2 Evaluación de riesgos de IA

La organización debe realizar evaluaciones de riesgos de IA de acuerdo con **6.1.2** en intervalos planificados o cuando se propongan o ocurran cambios significativos.

8.2 Evaluación de riesgos de IA

La organización debe conservar información documentada de los resultados de todas las evaluaciones de riesgos de IA.

8.3 Tratamiento de riesgos de IA

Contenido

La organización debe implementar el plan de tratamiento de riesgos de IA de acuerdo con **6.1.3** y verificar su eficacia.

8.3 Tratamiento de riesgos de IA

Cuando las evaluaciones de riesgos identifiquen nuevos riesgos que requieran tratamiento, debe realizarse un proceso de tratamiento de riesgos de acuerdo con **6.1.3** para estos riesgos.

8.3 Tratamiento de riesgos de IA

Cuando las opciones de tratamiento de riesgos definidas por el plan de tratamiento de riesgos no sean eficaces, estas opciones de tratamiento deben ser revisadas y validadas nuevamente siguiendo el proceso de tratamiento de riesgos de acuerdo con **6.1.3** y el plan de tratamiento de riesgos debe ser actualizado.

8.3 Tratamiento de riesgos de IA

La organización debe conservar información documentada de los resultados de todos los tratamientos de riesgos de IA.

8.4 Evaluación de impacto del sistema de IA

La organización debe realizar evaluaciones de impacto del sistema de IA de acuerdo con **6.1.4** en intervalos planificados o cuando se propongan cambios significativos.

8.4 Evaluación de impacto del sistema de IA

La organización debe conservar información documentada de los resultados de todas las evaluaciones de impacto del sistema de IA.

---

9 Evaluación del desempeño

9.1 Monitoreo, medición, análisis y evaluación

La organización debe determinar:

— qué necesita ser monitoreado y medido;

— los métodos para el monitoreo, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos;

9.1 Monitoreo, medición, análisis y evaluación

— cuándo se deben realizar el monitoreo y la medición;

— cuándo los resultados del monitoreo y la medición deben ser analizados y evaluados.

9.1 Monitoreo, medición, análisis y evaluación

La información documentada debe estar disponible como evidencia de los resultados.

9.1 Monitoreo, medición, análisis y evaluación

La organización debe evaluar el desempeño y la eficacia del sistema de gestión de IA.

9.2 Auditoría interna

9.2.1 General

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de IA:

a) cumple con:

1. los propios requisitos de la organización para su sistema de gestión de IA;

2. los requisitos de este documento;

9.2.1 General

Contenido

b) está implementado y mantenido eficazmente.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o más programas de auditoría que incluyan la frecuencia, métodos, responsabilidades, requisitos de planificación y elaboración de informes.

9.2.2 Programa de auditoría interna

Al establecer el programa de auditoría interna, la organización debe considerar la importancia de los procesos involucrados y los resultados de auditorías previas.

9.2.2 Programa de auditoría interna

La organización debe:

a) definir los objetivos, criterios y alcance de cada auditoría;

b) seleccionar auditores y realizar auditorías para asegurar la objetividad y la imparcialidad del proceso de auditoría;

9.2.2 Programa de auditoría interna

c) asegurar que los resultados de las auditorías se informen a los responsables pertinentes.

9.2.2 Programa de auditoría interna

La información documentada debe estar disponible como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.

9.3 Revisión por la dirección

9.3.1 General

La alta dirección debe revisar el sistema de gestión de IA de la organización, a intervalos planificados, para asegurar su conveniencia, adecuación y eficacia continuas.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir:

a) el estado de las acciones de revisiones previas por la dirección;

b) cambios en cuestiones externas e internas que sean relevantes para el sistema de gestión de IA;

9.3.2 Entradas de la revisión por la dirección

c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de IA;

d) información sobre el desempeño del sistema de gestión de IA, incluyendo tendencias en:

1. no conformidades y acciones correctivas;

9.3.2 Entradas de la revisión por la dirección

2. resultados de monitoreo y medición;

3. resultados de auditorías;

e) oportunidades de mejora continua.

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de IA.

9.3.3 Resultados de la revisión por la dirección

La información documentada debe estar disponible como evidencia de los resultados de las revisiones por la dirección.

10 Mejora

10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de IA.

10.2 No conformidad y acción correctiva

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según corresponda:

1. tomar acciones para controlarla y corregirla;

2. tratar las consecuencias.

10.2 No conformidad y acción correctiva

b) evaluar la necesidad de acciones para eliminar la(s) causa(s) de la no conformidad, con el fin de que no vuelva a ocurrir o que no ocurra en otro lugar, mediante:

1. revisar la no conformidad;

2. determinar las causas de la no conformidad;

10.2 No conformidad y acción correctiva

Contenido

3. determinar si existen no conformidades similares o si potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de cualquier acción correctiva tomada;

10.2 No conformidad y acción correctiva

e) realizar cambios en el sistema de gestión de IA, si es necesario.

10.2 No conformidad y acción correctiva

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

10.2 No conformidad y acción correctiva

Contenido

La información documentada debe estar disponible como evidencia de:

— la naturaleza de las no conformidades y cualquier acción posterior tomada;

— los resultados de cualquier acción correctiva.

Anexo A: Controles

Contenido

REQUISITOS ISO/IEC 42001:2023

4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

ANEXO A ISO/IEC 42001:2023

A.2 Políticas relacionadas con IA
A.3 Organización interna
A.4 Recursos para sistemas de IA
A.5 Evaluación de impactos de sistemas de IA
A.6 Ciclo de vida del sistema de IA
A.7 Datos para sistemas de IA
A.8 Información para partes interesadas de sistemas de IA
A.9 Uso de sistemas de IA
A.10 Relaciones con terceros y clientes

Anexo A: Cláusulas, Objetivos y Controles

9 GRUPOS

- Políticas relacionadas con IA
- Organización interna
- Recursos para sistemas de IA
- Evaluación de impactos de sistemas de IA
- Ciclo de vida del sistema de IA
- Datos para sistemas de IA
- Información para partes interesadas de sistemas de IA
- Uso de sistemas de IA
- Relaciones con terceros y clientes

38 CONTROLES

Anexo A: Controles

A.2 Políticas relacionadas con IA

A.2.2 Política de IA
A.2.3 Alineación con otras políticas organizacionales
A.2.4 Revisión de la política de IA

A.3 Organización interna

A.3.2 Roles y responsabilidades de IA

A.3.3 Reporte de preocupaciones

A.4 Recursos para sistemas de IA

A.4.2 Documentación de recursos

A.4.3 Recursos de datos

A.4.4 Recursos de herramientas

A.4.5 Recursos de sistema y computación

A.4.6 Recursos humanos

A.5 Evaluación de impactos de sistemas de IA

A.5.2 Proceso de evaluación de impacto del sistema de IA

A.5.3 Documentación de evaluaciones de impacto del sistema de IA

A.5.4 Evaluación del impacto del sistema de IA en individuos o grupos de individuos

A.5.5 Evaluación de impactos sociales de sistemas de IA

Anexo A: Controles

A.6 Ciclo de vida del sistema de IA

A.6.1 Gestión para el desarrollo del sistema de IA

A.6.1.2 Objetivos para el desarrollo responsable del sistema de IA

A.6.1.3 Procesos para el diseño y desarrollo responsable del sistema de IA

A.6.2 Ciclo de vida del sistema de IA

A.6.2.2 Requisitos y especificación del sistema de IA

A.6.2.3 Documentación del diseño y desarrollo del sistema de IA

A.6.2.4 Verificación y validación del sistema de IA

A.6.2.5 Despliegue del sistema de IA

A.6.2.6 Operación y monitoreo del sistema de IA

A.6.2.7 Documentación técnica del sistema de IA

A.6.2.8 Registro de eventos del sistema de IA

A.7 Datos para sistemas de IA

A.7.2 Datos para el desarrollo y mejora del sistema de IA

A.7.3 Adquisición de datos

A.7.4 Calidad de datos para sistemas de IA
A.7.5 Procedencia de los datos
A.7.6 Preparación de datos

A.8 Información para partes interesadas de sistemas de IA
A.8.2 Documentación del sistema e información para usuarios
A.8.3 Reporte externo
A.8.4 Comunicación de incidentes
A.8.5 Información para partes interesadas

A.9 Uso de sistemas de IA
A.9.2 Procesos para el uso responsable de sistemas de IA
A.9.3 Objetivos para el uso responsable del sistema de IA
A.9.4 Uso previsto del sistema de IA

A.10 Relaciones con terceros y clientes
A.10.2 Asignación de responsabilidades
A.10.3 Proveedores
A.10.4 Clientes

Anexo B: Guía de implementación para controles de IA

El **Anexo B** proporciona orientación para la implementación de los controles listados en **Anexo A (Tabla A.1)**.

La orientación de implementación tiene como propósito apoyar a las organizaciones en la aplicación práctica de los controles relacionados con el diseño, desarrollo, provisión o uso de sistemas de IA.

El Anexo B sigue la misma estructura de controles definida en el **Anexo A**.

Anexo B: Relación entre Anexo A y Anexo B

Los controles listados en **Anexo A** proporcionan objetivos de control y controles de referencia.

El **Anexo B** proporciona orientación de implementación para esos controles.

La orientación de implementación puede ayudar a las organizaciones a:

— comprender el propósito de los controles;
— considerar posibles enfoques para su implementación;
— adaptar los controles a su contexto organizacional.

B.2, B.3 y B.4 Guía de implementación para controles de IA

B.2 Políticas relacionadas con IA

Orientación para establecer, implementar y mantener políticas organizacionales relacionadas con el desarrollo o uso de sistemas de IA.

B.3 Organización interna

Orientación para definir responsabilidades organizacionales, estructuras de gobernanza y mecanismos para reportar preocupaciones relacionadas con sistemas de IA.

B.4 Recursos para sistemas de IA

Orientación para identificar, documentar y gestionar los recursos necesarios para el desarrollo, implementación y operación de sistemas de IA.

B.5 y B.6 Guía de implementación para controles de IA

B.5 Evaluación de impactos de sistemas de IA

Orientación para establecer procesos que permitan evaluar los impactos potenciales de sistemas de IA en individuos, grupos de individuos y la sociedad.

B.6 Ciclo de vida del sistema de IA

Orientación para definir criterios y procesos para las diferentes etapas del ciclo de vida del sistema de IA, incluyendo diseño, desarrollo, verificación, validación, despliegue y operación.

B.7 y B.8 Guía de implementación para controles de IA

B.7 Datos para sistemas de IA

Orientación para gestionar los datos utilizados en sistemas de IA, incluyendo adquisición, calidad, procedencia y preparación de datos.

B.8 Información para partes interesadas de sistemas de IA

Orientación para proporcionar información adecuada a las partes interesadas relevantes sobre el sistema de IA y sus posibles impactos.

B.9 y B.10 Guía de implementación para controles de IA

B.9 Uso de sistemas de IA

Orientación para asegurar que los sistemas de IA se utilicen de manera responsable y de acuerdo con las políticas organizacionales.

B.10 Relaciones con terceros y clientes

Orientación para gestionar responsabilidades, riesgos y obligaciones cuando terceros participan en el ciclo de vida de sistemas de IA.

Anexo C: Objetivos organizacionales relacionados con IA y fuentes de riesgo

El **Anexo C** proporciona ejemplos de posibles **objetivos organizacionales relacionados con sistemas de IA** y **fuentes de riesgo relacionadas con IA**.

Estos ejemplos pueden apoyar a las organizaciones en la identificación de:

— objetivos relacionados con el uso responsable de sistemas de IA;
— fuentes potenciales de riesgo asociadas con sistemas de IA.

NOTA

Los ejemplos proporcionados en este anexo no son exhaustivos y pueden variar según el contexto de la organización.

Anexo C: Ejemplos de objetivos organizacionales relacionados con IA

Contenido

Los objetivos organizacionales relacionados con sistemas de IA pueden incluir:

— mejorar la eficiencia o eficacia de procesos organizacionales;
— apoyar la toma de decisiones basada en datos;
— mejorar productos o servicios mediante el uso de IA;
— permitir nuevas capacidades organizacionales;
— mejorar la experiencia del usuario.

Estos objetivos pueden ser considerados al establecer **objetivos de IA (véase 6.2)**.

Anexo C: Ejemplos de fuentes de riesgo relacionadas con IA

Contenido

Las fuentes de riesgo relacionadas con sistemas de IA pueden incluir:

— calidad insuficiente de los datos utilizados por el sistema de IA;
— falta de transparencia o explicabilidad del sistema de IA;
— sesgos en los datos o modelos de IA;
— uso indebido del sistema de IA;
— cambios inesperados en el comportamiento del sistema de IA.

Estas fuentes de riesgo pueden ser consideradas en **evaluaciones de riesgo de IA (véase 6.1.2)**.

Anexo D: Uso del sistema de gestión de IA en diferentes dominios o sectores

El **Anexo D** describe cómo el sistema de gestión de IA puede aplicarse en diferentes dominios o sectores.

El sistema de gestión de IA puede ser utilizado por organizaciones en diversos contextos, incluyendo:

— desarrollo de sistemas de IA;
— provisión de productos o servicios que utilizan IA;
— uso de sistemas de IA desarrollados por terceros.

Anexo D: Aplicación del sistema de gestión de IA

El sistema de gestión de IA puede aplicarse a lo largo del ciclo de vida de los sistemas de IA.

Esto puede incluir actividades relacionadas con:

— diseño y desarrollo de sistemas de IA;
— integración de sistemas de IA en productos o servicios;
— operación y monitoreo de sistemas de IA.

Anexo D: Consideraciones sectoriales

Los requisitos y controles del sistema de gestión de IA pueden aplicarse en diferentes sectores.

Las organizaciones pueden adaptar la implementación del sistema de gestión de IA según:

— el sector o dominio en el que operan;
— el tipo de sistemas de IA utilizados;
— los requisitos regulatorios aplicables.

Módulo Internal Auditor

Auditorías internas del Sistema de Gestión de IA basadas en **ISO 19011**

Objetivo:

Comprender el proceso de auditoría interna para evaluar la conformidad y eficacia del **Sistema de Gestión de Inteligencia Artificial (SGIA)** basado en **ISO/IEC 42001**.

Fase 4. Auditorías Internas con Énfasis en Competencias de Auditor Líder

Basado en la Norma ISO 19011

Esta norma proporciona una guía para todos los tamaños y tipos de organizaciones y auditorías de diferentes alcances y escalas, incluidas aquellas realizadas por grandes equipos de auditoría, generalmente de organizaciones más grandes, y aquellas realizadas por auditores individuales, ya sea en organizaciones grandes o pequeñas.

Esta orientación debería adaptarse según corresponda al alcance, la complejidad y la escala del programa de auditoría.

Estructura de la ISO 19011:2018

Prefacio

Introducción

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Principios de auditoría
5. Administrar de un programa de auditoría
6. Realización de una auditoría
7. Competencia y evaluación de los auditores

Anexo A

Bibliografía

Alcance ISO 19011:2018

Este documento proporciona orientación sobre auditoría a sistemas de gestión, incluidos los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría.

Estas actividades incluyen las personas que administran el programa de auditoría, los auditores y los equipos de auditoría.

Es aplicable a todas las organizaciones que necesitan planificar y llevar a cabo auditorías internas o externas de los sistemas de gestión o administrar un programa de auditoría.

La aplicación de este documento a otros tipos de auditorías es posible, siempre que se otorgue una consideración especial a la competencia específica necesaria.

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.

Nota 1: las auditorías internas, a veces llamadas auditorías de primera parte, son realizadas por, o en nombre de, la organización misma.

Nota 2: Las auditorías externas incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre.

Tipos de Auditoría

TABLA 1 - DIFERENTES TIPOS DE AUDITORIA

Auditoría de Primera Parte	Auditoría de Segunda Parte	Auditoría de Tercera Parte
AUDITORÍA INTERNA	Auditoría de proveedor externo.	Auditoría de certificación y/o acreditación.
	Otra auditoría de parte interesada externa.	Auditoría legal, regulatoria y similar.

Tipos de Auditoría

A. Auditorías internas: a veces llamadas auditorías de primera parte son realizadas por o en nombre de la organización misma.

B. Auditorías externas: incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte.

1. **Auditorías de segunda parte:** se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre.

2. **Auditorías de tercera parte**: son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales.

Criterios de Auditoría

Conjunto de requisitos utilizados como referencia con respecto a los cuales se compara la evidencia objetiva.

Nota 1: Si los criterios de auditoría son legales (incluidos los requisitos legales o reglamentarios), las palabras "cumplimiento" o "incumplimiento" a menudo se utilizan en una conclusión de auditoría.

Nota 2: Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, etc.

Evidencia de la Auditoría

- La evidencia objetiva son los datos que respaldan la existencia o la verdad de algo.
- **Nota 1:** La evidencia objetiva se puede obtener a través de observación, medición, prueba o por otros medios.
- **Nota 2:** La evidencia objetiva para el propósito de la auditoría generalmente consiste en registros, declaraciones de hechos u otra información que son relevantes para los criterios de auditoría y verificables.

Resultados de la Auditoría

Los resultados de la evaluación de la evidencia de auditoría recopilada contra los criterios de auditoría.

- **Nota 1:** Los hallazgos de la auditoría indican conformidad o no conformidad.
- **Nota 2:** Los hallazgos de la auditoría pueden conducir a la identificación de riesgos, oportunidades de mejora o registro de buenas prácticas.

- **Nota 3:** en inglés, si los criterios de auditoría se seleccionan de entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o incumplimiento.

Resultados de la Auditoría

- Hallazgo de cumplimiento.
- Requisitos (norma, legal, reglamentario, contractual).
- El elemento se ajusta a la exigencia.
- La implantación corresponde a la intención.
- La implantación es eficaz.

Mejores prácticas

- Verificar los hechos verbales.
- Definir la naturaleza de la no conformidad con el auditado, detallando la evidencia de auditoría.
- Tomar notas y consultarlas posteriormente para realizar el reporte.
- Hacer un bosquejo del reporte de hallazgos durante la toma de información.
- Al finalizar cada jornada terminar en la revisión privada.

Conclusiones de la Auditoría

Resultado de una auditoría después de considerar los objetivos de auditoría y todos los resultados (hallazgos) de auditoría.

Cliente de la Auditoría

Organización o persona que solicita una auditoría.

• **Nota 1:** en el caso de la auditoría interna, el cliente de auditoría también puede ser el auditado o la persona(s) que administra el programa de auditoría. Las solicitudes de auditoría externa pueden provenir de fuentes tales como reguladores, partes contratantes o clientes potenciales o existentes.

Auditado

Organización en su totalidad o partes de ella siendo auditada.

Auditor

Persona que realiza una auditoría.

Equipo Auditor

Una o más personas que realizan una auditoría, apoyadas si es necesario por expertos técnicos.

•Nota 1: Un auditor del equipo de auditoría es designado como el líder del equipo de auditoría.

•Nota 2: El equipo de auditoría puede incluir auditores en capacitación.

Experto Técnico

Persona que proporciona conocimientos o experiencia específicos al equipo de auditoría.

•Nota 1: el conocimiento específico o experiencia se relaciona con la organización, la actividad, el proceso, el producto, el servicio, la disciplina que se auditará, el idioma o la cultura.

•Nota 2: Un experto técnico del equipo de auditoría no actúa como auditor.

Observador

Individuo que acompaña al equipo de auditoría pero que no actúa como auditor.

Guía

Persona designada por el auditado para asistir al equipo auditor.

Programa de Auditoría

Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Alcance de la Auditoría

Alcance de auditoría se refiere al alcance y límites de una auditoría.

El alcance de la auditoría generalmente incluye una descripción de las ubicaciones físicas y virtuales, funciones, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto.

Una ubicación virtual es cuando una organización realiza un trabajo o proporciona un servicio usando un entorno en línea que permite a las personas, independientemente de las ubicaciones físicas, ejecutar procesos.

Plan de Auditoría

Descripción de las actividades y los arreglos para una auditoría.

Conformidad

Cumplimiento de un requisito.

No Conformidad

Incumplimiento de un requisito.

Pruebas de Auditoría

Registros, declaraciones de hechos u otra información, que sean relevantes para los criterios de auditoría y verificables.

Métodos de Auditoría

ALCANCE DE LA PARTICIPACIÓN ENTRE EL AUDITOR Y EL AUDITADO	Ubicación del Auditor	
	En el sitio	**Remota**
Interacción Humana	- Realización de entrevistas. - Completar listas de verificación y cuestionarios con participación del auditado. - Realización de una revisión de documentos con participación del auditado. - Muestreo.	**A través de comunicación interactiva significa:** - Realización de entrevistas. - Observar el trabajo realizado con la guía remota. - Completando listas de verificación y cuestionarios. - Realización de revisión de documentos con participación de los propietarios.
Sin Interacción Humana	- Realización de revisión de documentos (por ejemplo: registros, análisis de datos). - Observando el trabajo realizado. - Llevando a cabo una visita in-situ. - Completando listas de verificación. - Muestreo (por ejemplo: productos).	- Realización de revisión de documentos (por ejemplo: registros, análisis de datos). - Observar el trabajo realizado a través de medios de vigilancia, teniendo en cuenta los requisitos sociales, estatutarios y normativos. - Análisis de datos.

Las actividades de auditoría en el sitio se realizan en la ubicación del auditado. Las actividades de auditoría remota se realizan en cualquier lugar que no sea la ubicación del auditado, independientemente de la distancia. Las actividades de auditoría interactiva, implican la interacción entre el personal del auditado y el equipo de auditoría. Las actividades de auditoría no interactiva no implican interacción humana con las personas que representan al auditado, pero si implican la interacción con el equipo, las instalaciones y la documentación.

Cláusula 4: Principios de Auditoría

1. **Integridad:** la base del profesionalismo
2. **Presentación justa:** la obligación de informar veraz y exactamente
3. **Debido cuidado profesional:** la aplicación de la diligencia y el juicio en la auditoría
4. **Confidencialidad:** seguridad de la información
5. **Independencia:** la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría
6. **Enfoque basado en la evidencia:** el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático
7. **Enfoque basado en el riesgo:** un enfoque de auditoría que considera riesgos y oportunidades

Cláusula 4: Principios de Auditoría

Integridad: la base del profesionalismo

Los auditores y la (s) persona (s) que administran un programa de auditoría deberían:

a) Realizar su trabajo de forma ética, con honestidad y responsabilidad.

b) Solo realizar actividades de auditoría si es competente para hacerlo.

c) Realizar su trabajo de manera imparcial, es decir, seguir siendo justo e imparcial en todos sus tratos.

d) Ser sensible a cualquier influencia que pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

Cláusula 4: Principios de Auditoría

Presentación justa: la obligación de informar veraz y exactamente

Los hallazgos de la auditoría, las conclusiones de auditoría y los informes de auditoría deberían reflejar de manera veraz y precisa las actividades de auditoría. Se deberían informar los obstáculos significativos encontrados durante la auditoría y las opiniones divergentes no resueltas entre el equipo de auditoría y el auditado. La comunicación debería ser veraz, precisa, objetiva, oportuna, clara y completa.

Cláusula 4: Principios de Auditoría

Debido cuidado profesional: la aplicación de la diligencia y el juicio en la auditoría

Los auditores deberían tener el debido cuidado de acuerdo con la importancia de la tarea que realizan y la confianza depositada en ellos por el cliente de auditoría y otras partes interesadas. Un factor importante para llevar a cabo su trabajo con la debida atención profesional es tener la capacidad de emitir juicios razonados en todas las situaciones de auditoría.

Cláusula 4: Principios de Auditoría

Confidencialidad: seguridad de la información

Los auditores deberían ejercer discreción en el uso y la protección de la información adquirida en el desempeño de sus funciones. La información de auditoría no debería ser utilizada de manera inapropiada para beneficio personal por el auditor o el cliente de auditoría, o de una manera perjudicial para los intereses legítimos del auditado. Este concepto incluye el manejo adecuado de información sensible o confidencial.

Cláusula 4: Principios de Auditoría

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 auditada siempre que sea posible y, en todos los casos, deberían actuar de forma tal que no estén sujetos a prejuicios ni a conflictos de intereses. Para las auditorías internas, los auditores deberían ser independientes de la función que se está auditando, si es posible. Los auditores deberían mantener la objetividad durante todo el proceso de auditoría para garantizar que los hallazgos y conclusiones de la auditoría se basen solo en la evidencia de auditoría.

Para las organizaciones pequeñas, puede que los auditores internos no sean totalmente independientes de la actividad que se audita, pero se deberían hacer todos los esfuerzos para eliminar el sesgo y alentar la objetividad.

Cláusula 4: Principios de Auditoría

Enfoque basado en la evidencia: el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático

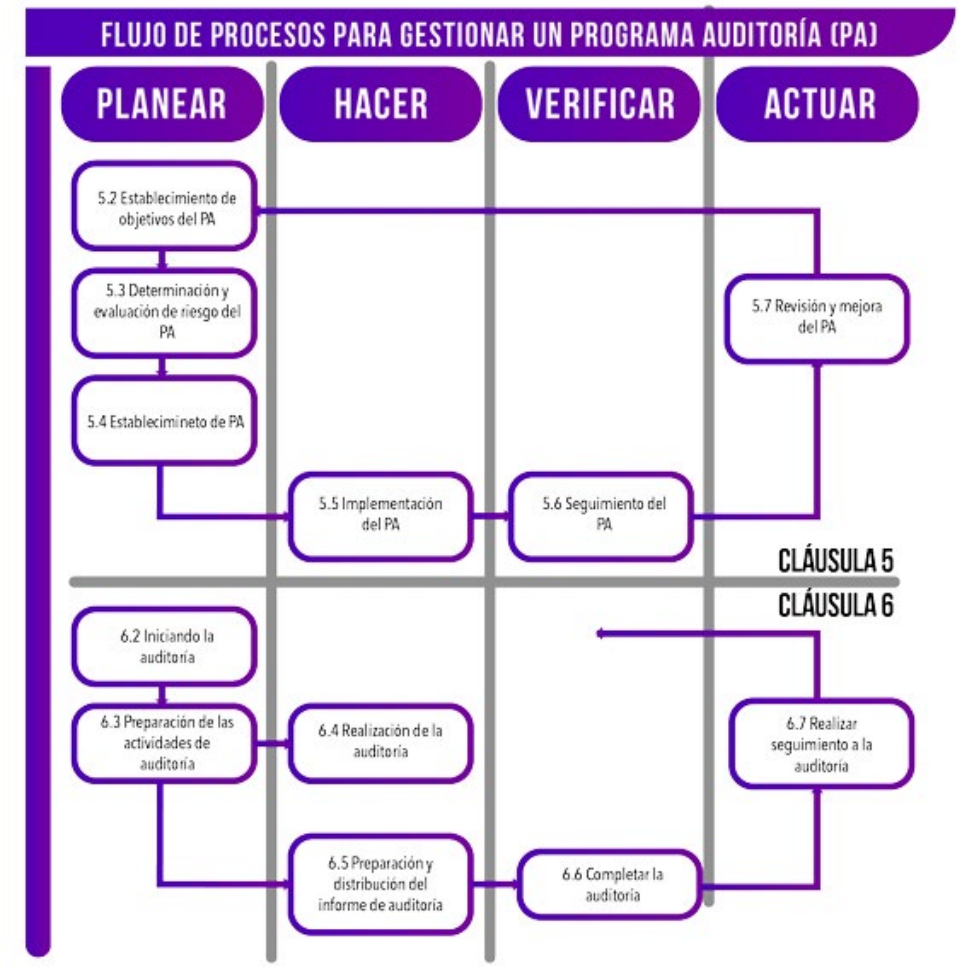
La evidencia de auditoría debería ser verificable. En general, debería basarse en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un tiempo finito y con recursos limitados. Se debería aplicar un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que se puede depositar en las conclusiones de la auditoría.

Cláusula 4: Principios de Auditoría

Enfoque basado en el riesgo: un enfoque de auditoría que considera riesgos y oportunidades

El enfoque basado en el riesgo debería influir sustancialmente en la planificación, conducción y presentación de informes de las auditorías para garantizar que las auditorías se centren en asuntos que son importantes para el cliente de auditoría y para lograr los objetivos del programa de auditoría.

Cláusula 5: Programa de Auditoría



NOTA 1: Esta figura ilustra la aplicación Planear – Hacer – Verificar – Actuar, en este documento.

NOTA 2: La numeración de cláusulas/subcláusulas se refiere a las cláusulas/subcláusulas relevantes de este documento.

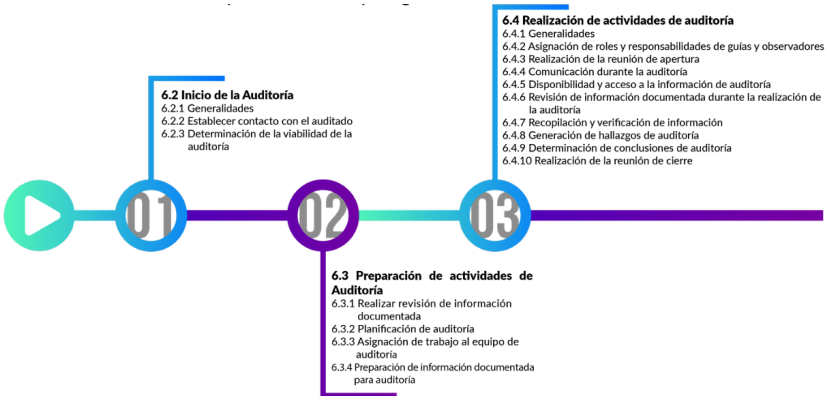
Figura 1: Flujo de proceso para la gestión de un programa de auditoría.

Cláusula 5: Programa de Auditoría

AUDITORÍAS	MES 1	MES 2	MES 3	MES 4	MES 5
Auditoría 1					
Auditoría 2					
Auditoría 3					

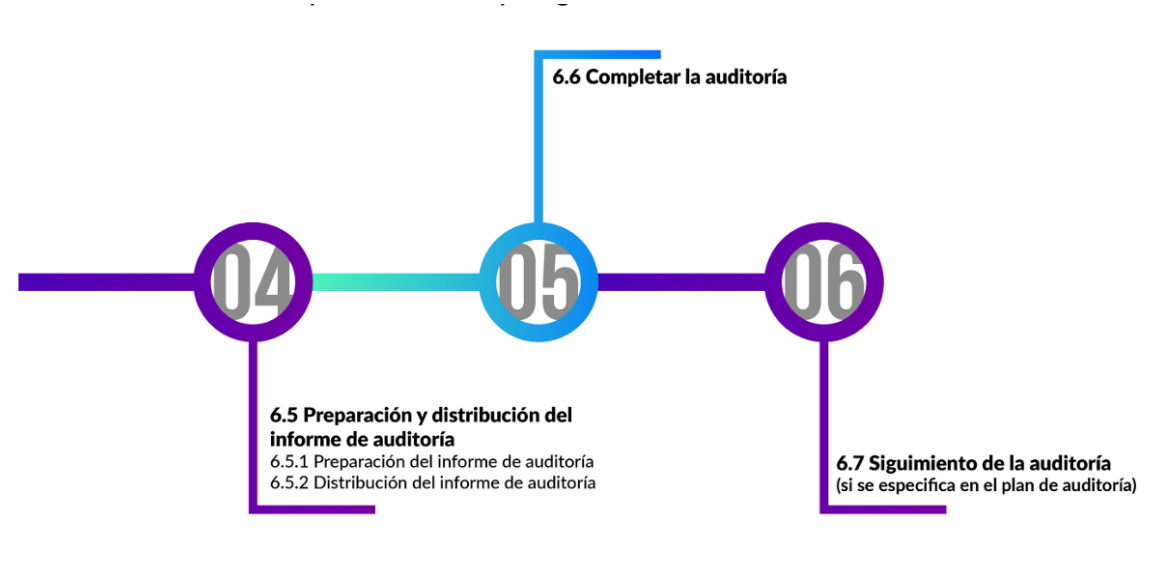
Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.



Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.



Cláusula 6: Actividades de la Auditoría

El líder del equipo auditor debería: Realizar reuniones informativas del equipo auditor, cuando sea apropiado, para distribuir las asignaciones de trabajo y decidir los posibles cambios.

Cláusula 7: Competencia y Evaluación de los Auditores

Esta cláusula trata las competencias de los auditores al realizar una auditoría. Los auditores deben:

• Poseer cualidades personales, tales como diplomacia, sinceridad, percepción, persistencia, etc. para que la auditoría se realice en forma profesional y correcta a la vez

• Poseer conocimientos genéricos y habilidades tales como:

- Aplicar principios, procedimientos y técnicas de auditoría.
- Planificar y organizar el trabajo en forma eficaz.
- Conocer los códigos, leyes y normativas locales, regionales y nacionales.

Cláusula 7: Competencia y Evaluación de los Auditores

Poseer un adecuado nivel de educación, experiencia laboral, capacitación como auditor y experiencia en auditorías.

Mantener y mejorar en forma continua sus habilidades y competencias.

Métodos para Evaluar a los Auditores

MÉTODO DE EVALUACIÓN	OBJETIVOS	EJEMPLOS
REVISIÓN DE REGISTROS	Verificar los antecedentes del auditor.	Análisis de registros de educación, capacitación, empleo, credenciales profesionales y experiencia en auditoría.
RETROALIMENTACIÓN	Obtener / proporcionar información sobre cómo se percibe el desempeño del auditor.	Encuestas, cuestionarios, referencias personales, testimonios, reclamos, evaluación de desempeño, revisión por pares.
ENTREVISTA	Evaluar el comportamiento profesional deseado y las habilidades de comunicación. Verificar la información y probar el conocimiento y adquirir información adicional.	Entrevistas personales.
OBSERVACIÓN	Evaluar el comportamiento profesional deseado y la capacidad de aplicar los conocimientos y las habilidades.	Role playing, auditorías atestiguadas, desempeño en el trabajo.
PRUEBAS	Evaluar el comportamiento deseado, el conocimiento, las habilidades y su aplicación.	Exámenes orales y escritos, pruebas psicométricas.
REVISIÓN POSTERIOR A LA AUDITORÍA	Proporcionar información sobre el desempeño del auditor durante las actividades de auditoría, indentificar fortalezas y oportunidades de mejora.	Revisión del informe de auditoría, entrevistas con el lídes del equipo de auditoría, el equio de auditoría y si corresponde, retroalimentación del auditado.

Cláusula 7: Atributos Personales

a) Ético, es decir, justo, veraz, sincero, honesto y discreto

b) De mente abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos

c) Diplomático, es decir, discreto al tratar con individuos.

d) Observador, es decir, observando activamente el entorno físico y las actividades.

e) Perceptivo, es decir, consciente de y capaz de comprender situaciones.

f) Versátil, es decir, capaz de adaptarse fácilmente a diferentes situaciones.

g) Tenaz, es decir persistente y enfocado en alcanzar objetivos.

Cláusula 7: Atributos Personales

h. Decisivo, es decir, capaz de llegar a conclusiones oportunas basadas en el razonamiento lógico y el análisis.

i. Autosuficiente, es decir, capaz de actuar y funcionar independientemente mientras interactúa efectivamente con otros.

j. Capaz de actuar con fortaleza, es decir, capaz de actuar de manera responsable y ética, aunque estas acciones no siempre sean populares y en ocasiones pueden dar lugar a desacuerdos o confrontaciones.

k. Abierto a la mejora, es decir, dispuesto a aprender de las situaciones.

l. Culturalmente sensible, es decir, atento y respetuoso con la cultura del auditado.

m. Colaborador, es decir, interacción efectiva con otros, incluidos los miembros del equipo de auditoría y el personal del auditado

Cláusula 7: Conocimientos Genéricos y Habilidades

a) Los auditores deberían tener conocimiento y habilidades en las áreas que se detallan a continuación: **Principios, procesos y métodos de auditoría:** el conocimiento y las habilidades en esta área le permiten al auditor asegurar que las auditorías se realicen de manera consistente y sistemática.

Un auditor debería ser capaz de:

• Comprender los tipos de riesgos y oportunidades asociados con la auditoría y los principios del enfoque de auditoría basado en el riesgo.
• Planificar y organizar el trabajo de manera efectiva.
• Realizar la auditoría dentro del cronograma acordado.
• Priorizar y enfocarse en asuntos importantes.
• Comunicarse de manera efectiva, oralmente y por escrito (ya sea personalmente o mediante el uso de intérpretes).
• Recopilar información mediante entrevistas efectivas, escuchar, observar y revisar información documentada, incluidos registros y datos.

Cláusula 7: Conocimientos Genéricos y Habilidades

Un auditor debería ser capaz de:

• Comprender la idoneidad y las consecuencias del uso de técnicas de muestreo para la auditoría.
• Entender y considerar las opiniones de los expertos técnicos.
• Auditar un proceso de principio a fin, incluidas las interrelaciones con otros procesos y diferentes funciones, según corresponda.
• Verificar la relevancia y exactitud de la información recopilada.
• Confirmar la suficiencia e idoneidad de la evidencia de auditoría para respaldar los hallazgos y conclusiones de la auditoría.
• Evaluar aquellos factores que pueden afectar la confiabilidad de los hallazgos y

conclusiones de la auditoría.
• Documentar las actividades de auditoría y los hallazgos de auditoría, y preparar informes.
• Mantener la confidencialidad y seguridad de la información.

Cláusula 7: Conocimientos Genéricos y Habilidades

b) **Normas del sistema de gestión y otras referencias:** el conocimiento y las habilidades en esta área le permiten al auditor comprender el alcance de la auditoría y aplicar criterios de auditoría, y deberían cubrir lo siguiente:

• Normas del sistema de gestión u otros documentos normativos u orientativos/de apoyo utilizados para establecer criterios o métodos de auditoría.
• La aplicación de los estándares del sistema de gestión por el auditado y otras organizaciones.
• Relaciones e interacciones entre los procesos del sistema de gestión.
• Comprender la importancia y la prioridad de múltiples estándares o referencias
• Aplicación de estándares o referencias a diferentes situaciones de auditoría.

Cláusula 7: Conocimientos Genéricos y Habilidades

c) **La organización y su contexto:** el conocimiento y las habilidades en esta área le permiten al auditor comprender la estructura, propósito y gestión del auditado y deberían cubrir lo siguiente:

• Necesidades y expectativas de las partes interesadas pertinentes
• Tipo de organización, gobernanza, tamaño, estructura, funciones y relaciones
• Conceptos generales de gestión y procesos empresariales relacionados
• Aspectos culturales y sociales del auditado

Cláusula 7: Conocimientos Genéricos y Habilidades

d) Requisitos reglamentarios y legales aplicables y otros requisitos: el conocimiento y las
habilidades en esta área le permiten al auditor conocer y trabajar dentro de los requisitos de la organización. Los conocimientos y habilidades específicos de la jurisdicción o de las actividades, procesos, productos y servicios del auditado deberían cubrir lo siguiente:

- Requisitos legales y reglamentarios, así como sus agencias de gobierno
- Terminología jurídica básica
- Contratación y responsabilidad

NOTA: La conciencia de los requisitos legales y reglamentarios no implica pericia legal y una auditoría del sistema de gestión no debería tratarse como una auditoría de cumplimiento legal.

Cláusula 7: Conocimientos Genéricos y Habilidades

La 19011 lo define como arreglos para un conjunto de una o más auditorías planificadas para un marco de tiempo específico y dirigidas hacia un propósito específico.

- Un programa de auditoría puede incluir una o más auditorías, dependiendo del tamaño, la
naturaleza y la complejidad de la organización que va a ser auditada.

- El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza del
auditado, así como en la naturaleza, funcionalidad, complejidad, el tipo de riesgos y oportunidades, y el nivel de madurez de los sistemas de gestión a ser auditados

• Para comprender el contexto del auditado, el programa de auditoría debería tener en cuenta:
• Objetivos organizacionales.
• Cuestiones externas e internas relevantes.
• Las necesidades y expectativas de las partes interesadas pertinentes.
• Requisitos de confidencialidad y SGIA.

Establecimiento de Objetivos del Programa de Auditoría

El cliente de auditoría debería asegurarse de que los objetivos del programa de auditoría se establezcan para dirigir la planificación y la realización de auditorías, y debería garantizar que el programa de auditoría se implemente de manera efectiva.

Los objetivos del programa de auditoría deberían ser coherentes con la orientación estratégica y los objetivos y la política del sistema de gestión de soporte del cliente de auditoría.

Estos objetivos pueden basarse en la consideración de lo siguiente:

a) Las necesidades y expectativas de las partes interesadas pertinentes, tanto externas como internas.

b) Características y requisitos de procesos, productos, servicios y proyectos, y cualquier cambio en ellos.

c) Requisitos del sistema de gestión.

d) Necesidad de evaluación de proveedores externos.

e) El nivel de rendimiento y el nivel de madurez del sistema o sistemas de gestión del auditado, como se refleja en los indicadores de rendimiento relevantes (por ejemplo, KPI's), la ocurrencia de no conformidades, incidentes o quejas de las partes interesadas.

f) Identificó riesgos y oportunidades para el auditado.

g) Resultados de auditorías anteriores.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Existen riesgos y oportunidades relacionados con el contexto del auditado que pueden asociarse con un programa de auditoría y pueden afectar el logro de sus objetivos.

La persona responsable del programa de auditoría **debería considerar los riesgos** durante el desarrollo del programa:

a) Planificación, por ejemplo; no establecer los objetivos de auditoría relevantes y determinar el alcance, el número, la duración, las ubicaciones y el cronograma de las auditorías.

b) Recursos, por ejemplo; permitir tiempo, equipo y/o capacitación insuficientes para desarrollar el programa de auditoría o realizar una auditoría

c) Selección del equipo de auditoría, por ejemplo; competencia global insuficiente para realizar auditorías de manera efectiva

d) Comunicación, por ejemplo; procesos/canales de comunicación externos/internos ineficaces

---

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

e) Implementación, por ejemplo; coordinación ineficaz de las auditorías dentro del programa de auditoría, o no considerar la seguridad y confidencialidad de la información.

f) Control de la información documentada, por ejemplo; la determinación ineficaz de la información documentada necesaria requerida por los auditores y las partes interesadas pertinentes; la falta de protección adecuada de los registros de auditoría para demostrar la eficacia del programa de auditoría.

g) Supervisar, revisar y mejorar el programa de auditoría, por ejemplo; seguimiento ineficaz de los resultados del programa de auditoría.

h) Disponibilidad y cooperación del auditado y disponibilidad de evidencia para ser muestreada.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Las oportunidades para mejorar el programa de auditoría pueden incluir:

a) Permitir múltiples auditorías en una sola visita.

b) Minimizar el tiempo y las distancias que viajan al sitio.

c) Hacer coincidir el nivel de competencia del equipo de auditoría con el nivel de competencia necesario para alcanzar los objetivos de la auditoría.

d) Alinear las fechas de auditoría con la disponibilidad del personal clave del auditado.

Establecimiento del Programa de Auditoría

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

a) Establecer la extensión del programa de auditoría de acuerdo con los objetivos relevantes y cualquier restricción conocida.

b) Determinar los problemas externos e internos, y los riesgos y oportunidades que pueden afectar el programa de auditoría, e implementar acciones para abordarlos,

integrando estas acciones en todas las actividades de auditoría relevantes, según corresponda.

c) Garantizar la selección de los equipos de auditoría y la competencia general para las actividades de auditoría mediante la asignación de funciones, responsabilidades y autoridades, y el apoyo al liderazgo, según corresponda.

Establecimiento del Programa de Auditoría

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

d) Establecer todos los procesos relevantes, incluidos los procesos para:

• La coordinación y programación de todas las auditorías dentro del programa de auditoría.

• El establecimiento de objetivos de auditoría, alcance (s) y criterios de las auditorías,
determinación de los métodos de auditoría y selección del equipo de auditoría.
• Evaluación de auditores.
• El establecimiento de procesos de comunicación externa e interna, según corresponda
• La resolución de disputas y el manejo de quejas.
• Seguimiento de auditoría si corresponde.

• Informar al cliente de auditoría y a las partes interesadas pertinentes, según corresponda

---

Establecimiento del Programa de Auditoría

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

e) Determinar y garantizar la provisión de todos los recursos necesarios
f) Garantizar que se prepare y mantenga la información documentada apropiada, incluidos los registros del programa de auditoría.

g) Monitorear, revisar y mejorar el programa de auditoría.

h) Comunicar el programa de auditoría al cliente de auditoría y, según corresponda, a las partes interesadas pertinentes.

Las personas que gestionan el programa de auditoría deberían solicitar su aprobación al cliente de auditoría.

Competencia de (los) Individuo(s) que Gestiona(n) el Programa de Auditoría

La(s) persona(s) que gestiona(n) el programa de auditoría deberían tener la competencia necesaria para gestionar el programa, sus riesgos y oportunidades asociados y los problemas externos e internos de manera efectiva y eficiente, incluido el conocimiento de:

a) Principios de auditoría, métodos y procesos.

b) Normas del sistema de gestión, otras normas pertinentes y documentos de referencia / orientación.

c) Información sobre el auditado y su contexto (por ejemplo, asuntos externos/internos, partes interesadas relevantes y sus necesidades y expectativas, actividades comerciales, productos, servicios y procesos del auditado.

d) Requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades comerciales del auditado.

Establecer el Alcance del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían determinar el alcance del programa de auditoría. Esto puede variar según la información proporcionada por el auditado con respecto a su contexto. Otros factores que impactan en el alcance del programa de auditoría:

a) El objetivo, el alcance y la duración de cada auditoría y la cantidad de auditorías que se llevarán a cabo, el método de notificación y, si corresponde, el seguimiento de la auditoría.

b) Las normas del sistema de gestión u otros criterios aplicables.

c) El número, la importancia, la complejidad, la similitud y la ubicación de las actividades a auditar.

Establecer el Alcance del Programa de Auditoría

d) Aquellos factores que influyen en la efectividad del sistema de gestión.

e) Los criterios de auditoría aplicables, tales como los arreglos planificados para las normas del sistema de gestión pertinentes, los requisitos legales y reglamentarios y otros requisitos con los que la organización está comprometida.

f) Resultados de auditorías internas o externas previas y revisiones de la dirección, si corresponde.

g) Resultados de una revisión previa del programa de auditoría.

h) Problemas lingüísticos, culturales y sociales.

i) Las preocupaciones de las partes interesadas, tales como las quejas de los clientes, el incumplimiento de los requisitos legales y reglamentarios y otros requisitos con los que la organización se compromete, o los problemas de la cadena de suministro.

Establecer el Alcance del Programa de Auditoría

j) Cambios significativos en el contexto del auditado o sus operaciones y riesgos y oportunidades relacionados.

k) Disponibilidad de tecnologías de información y comunicación para respaldar las actividades de auditoría, en particular el uso de métodos de auditoría remota.

l) La ocurrencia de eventos internos y externos, tales como no conformidades de productos o servicios, fugas de seguridad de la información, incidentes de salud y seguridad, actos delictivos o incidentes ambientales.

m) Riesgos y oportunidades comerciales, incluidas las acciones para abordarlos.

Determinar los Recursos del Programa de Auditoría

Al determinar los recursos para el programa de auditoría, las personas que gestionan el programa de auditoría deberían considerar:

a) Los recursos financieros y de tiempo necesarios para desarrollar, implementar, administrar y mejorar las actividades de auditoría.

b) Métodos de auditoría.

c) La disponibilidad individual y general de auditores y expertos técnicos que posean las competencias apropiadas para los objetivos particulares del programa de auditoría.

d) La extensión del programa de auditoría y los riesgos y oportunidades del programa de auditoría.

e) Tiempo de viaje y costo, alojamiento y otras necesidades de auditoría.

Determinar los Recursos del Programa de Auditoría

f) El impacto de las diferentes zonas horarias.

g) La disponibilidad de tecnologías de información y comunicación (por ejemplo, los recursos técnicos necesarios para establecer una auditoría remota utilizando tecnologías que admiten la colaboración remota).

h) La disponibilidad de cualquier herramienta, tecnología y equipo requerido.

i) La disponibilidad de la información documentada necesaria, según se determine durante el establecimiento del programa de auditoría.

j) Los requisitos relacionados con la instalación, incluidos los espacios de seguridad y el equipo (por ejemplo, equipo de protección personal entre otras).

Implementación del Programa de Auditoría

a) Comunicar las partes pertinentes del programa de auditoría, incluidos los riesgos y oportunidades, a las partes interesadas pertinentes e informarles periódicamente de su progreso, utilizando los canales de comunicación externos e internos establecidos

b) Definir objetivos, alcance y criterios para cada auditoría individual.

c) Seleccionar métodos de auditoría.

d) Coordinar y programar auditorías y otras actividades relevantes para el programa de
auditoría.

e) Garantizar que los equipos de auditoría tengan la competencia necesaria

f) Proporcionar los recursos individuales y globales necesarios a los equipos de auditoría

g) Garantizar la realización de auditorías de acuerdo con el programa de auditoría, gestionando todos los riesgos, oportunidades y problemas operativos (es decir, eventos inesperados), tal como surgen durante el despliegue del programa.

h) Garantizar que la información documentada relevante con respecto a las actividades de auditoría se gestiona y mantiene de forma adecuada.

i) Definir e implementar los controles operativos necesarios para la supervisión del programa de auditoría.

j) Revisar el programa de auditoría para identificar oportunidades para su mejora.

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

Cada auditoría individual debería basarse en objetivos de auditoría definidos, alcance y criterios. Estos deberían ser consistentes con los objetivos generales del programa de auditoría.

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

a) Determinación del grado de conformidad del sistema de gestión a ser auditado, o partes de él, con los criterios de auditoría.

b) Evaluación de la capacidad del sistema de gestión para ayudar a la organización a cumplir los requisitos legales y reglamentarios pertinentes y otros requisitos con los que la organización está comprometida.

c) Evaluación de la efectividad del sistema de gestión para alcanzar los resultados esperados.

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

d) Identificación de oportunidades para la mejora potencial del sistema de gestión.

e) Evaluación de la idoneidad y adecuación del sistema de gestión con respecto al contexto y la dirección estratégica del auditado.

f) Evaluación de la capacidad del sistema de gestión para establecer y alcanzar objetivos y abordar de manera efectiva los riesgos y oportunidades, en un contexto cambiante, incluida la implementación de las acciones relacionadas.

El alcance de la auditoría debería ser coherente con el programa de auditoría y los objetivos de auditoría.

Selección y Determinación de Métodos de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) seleccionar y determinar los métodos para llevar a cabo eficazmente y de manera eficiente una auditoría, dependiendo de los objetivos de auditoría definidos, el alcance y criterios.

Las auditorías pueden realizarse en el sitio, de forma remota o como una combinación. El uso de estos métodos debería estar adecuadamente equilibrado, en función de, entre otros, la consideración de los riesgos y oportunidades asociados.

Si un auditado opera dos o más sistemas de gestión de diferentes disciplinas, se pueden incluir auditorías combinadas en el programa de auditoría.

Selección de los Miembros del Equipo de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) nombrar a los miembros del equipo de auditoría, incluyendo el líder del equipo y cualquier

expertos técnicos necesarios para la auditoría específica.

Se debería seleccionar un equipo de auditoría, teniendo en cuenta la competencia necesaria para alcanzar los objetivos de la auditoría individual dentro del alcance definido. Si solo hay un auditor, el auditor debería realizar todas las tareas aplicables de un líder del equipo de auditoría.

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

Las personas que gestionan el programa de auditoría deberían asignar la responsabilidad de llevar a cabo la auditoría individual a un líder del equipo de auditoría.

La asignación debería hacerse con suficiente tiempo antes de la fecha programada de la auditoría, a fin de garantizar la planificación efectiva de la auditoría.

Para que la auditoría se lleve a cabo eficazmente, se deberá proporcionar al auditor líder información sobre:

a) Objetivos de auditoría.

b) Criterios de auditoría y cualquier información documentada relevante.

c) Alcance de la auditoría, incluida la identificación de la organización y sus funciones y procesos a auditar.

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

d) Procesos de auditoría y métodos asociados.
e) Composición del equipo de auditoría.
f) Los datos de contacto del auditado, las ubicaciones, el marco temporal y la duración de las actividades de auditoría que se llevarán a cabo.

g) Los recursos necesarios para llevar a cabo la auditoría.

h) Información necesaria para evaluar y abordar los riesgos y oportunidades identificados para el logro de los objetivos de la auditoría.

i) Información que respalda al (los) líder (es) del equipo de auditoría en sus interacciones con el auditado para la efectividad del programa de auditoría.

Gestión de los Resultados del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar que se realicen las siguientes actividades:

a) Evaluación del logro de los objetivos para cada auditoría dentro del programa de auditoría.

b) Revisión y aprobación de informes de auditoría sobre el cumplimiento del alcance y los
objetivos de la auditoría.

c) Revisión de la efectividad de las acciones tomadas para abordar los hallazgos de auditoría.

d) Distribución de informes de auditoría a las partes interesadas pertinentes.

e) Determinación de la necesidad de cualquier auditoría de seguimiento.

La persona que administra el programa de auditoría debería considerar, cuando corresponda:

• Comunicar los resultados de auditoría y las mejores prácticas a otras áreas de la organización.

• Las implicaciones para otros procesos.

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que administran el programa de auditoría deberían garantizar que los registros de auditoría se generen, administren y mantengan para demostrar la implementación del programa de auditoría.

Los registros pueden incluir lo siguiente:

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

• Calendario de auditorías

• Objetivos y alcance del programa de auditoría

• Aquellos que abordan los riesgos y oportunidades del programa de auditoría, y los problemas externos e internos relevantes.

• Revisiones de la efectividad del programa de auditoría.

Administrar y Mantener los Registros del Programa de Auditoría

b) Registros relacionados con cada auditoría, tales como:

• Planes de auditoría e informes de auditoría

• Evidencia de auditoría objetiva y hallazgos.

• Informes de no conformidad.

• Correcciones e informes de acciones correctivas.

• Informes de seguimiento de auditoría.

c) Registros relacionados con el equipo de auditoría que cubren temas tales como:
• Evaluación de competencia y desempeño de los miembros del equipo de auditoría-
• Criterios para la selección de equipos de auditoría y miembros del equipo y formación de equipos de auditoría.

• Mantenimiento y mejora de la competencia.

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar la evaluación de:
a) Sí se están cumpliendo los cronogramas y si se están logrando los objetivos del programa de auditoría.

b) El desempeño de los miembros del equipo de auditoría, incluido el líder del equipo de auditoría y los expertos técnicos.

c) La capacidad de los equipos de auditoría para implementar el plan de auditoría.

d) Retroalimentación de clientes de auditoría, auditados, auditores, expertos técnicos y otras
partes relevantes.

e) Suficiencia y adecuación de la información documentada en todo el proceso de auditoría.

Revisión y Mejora del Programa de Auditoría

Las personas que gestionan el programa de auditoría y el cliente de auditoría deberían revisar el programa de auditoría para evaluar si se han alcanzado sus objetivos.

La revisión del programa de auditoría debería considerar lo siguiente:

a) Resultados y tendencias del seguimiento del programa de auditoría.

b) Conformidad con los procesos del programa de auditoría e información documentada
relevante.

c) La evolución de las necesidades y expectativas de las partes interesadas pertinentes.

d) Registros del programa de auditoría.

e) Métodos de auditoría alternativos o nuevos.

f) Métodos alternativos o nuevos para evaluar a los auditores.

g) Efectividad de las acciones para abordar los riesgos y oportunidades, y problemas internos y externos asociados con el programa de auditoría.

h) Cuestiones de confidencialidad y IA relacionadas con el programa de auditoría.

Establecer Contacto con el Auditado

Es responsabilidad del auditor líder.

Propósito

a) Confirmar los canales de comunicación con los representantes del auditado.

b) Confirmar la autoridad para realizar la auditoría.

c) Proporcionar información relevante sobre los objetivos, el alcance, los criterios, los métodos y la composición del equipo de auditoría, incluidos los expertos técnicos.

d) Solicitar acceso a información relevante para fines de planificación, incluida información
sobre los riesgos y oportunidades que la organización ha identificado y cómo se abordan.

e) Determinar los requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades, procesos, productos y servicios del auditado.

Establecer Contacto con el Auditado

f) Confirmar el acuerdo con el auditado sobre el alcance de la divulgación y el tratamiento de la información confidencial.

g) Hacer arreglos para la auditoría incluyendo el cronograma.
h) Determinar los arreglos específicos de ubicación para el acceso, la salud y la seguridad, la confidencialidad u otros.

i) Acordar la asistencia de los observadores y la necesidad de guías o intérpretes para el equipo de auditoría.

j) Determinar cualquier área de interés, preocupación o riesgo para el auditado en relación con la auditoría específica.

k) Resolver problemas relacionados con la composición del equipo de auditoría con el auditado o el cliente de auditoría.

Determinación de la Viabilidad de la Auditoría

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

a) Información suficiente y apropiada para planificar y llevar a cabo la auditoría.
b) Cooperación adecuada del auditado.
c) Tiempo y recursos adecuados para realizar la auditoría.

Realizar Revisión de Información Documentada

Debería revisarse la documentación para:

• Recopilar información para comprender las operaciones del auditado y preparar las
actividades de auditoría y los documentos de trabajo de auditoría aplicables (ver 6.3.4), por
ejemplo; en procesos y funciones

• Establecer una visión general del alcance de la información documentada para determinar la posible conformidad con los criterios de auditoría y detectar posibles áreas de preocupación, como deficiencias, omisiones o conflictos.

La información documentada debería incluir, pero no limitarse a:
• Documentos y registros del sistema de gestión

• Informes de auditoría anteriores

La revisión debería tener en cuenta el contexto de la organización del auditado, incluidos su tamaño, naturaleza y complejidad, y sus riesgos y oportunidades relacionados. También debería tener en cuenta el alcance, los criterios y los objetivos de la auditoría.

Planificación de Auditoría

Enfoque basado en el riesgo para la planificación

El líder del equipo de auditoría debería adoptar un enfoque basado en el riesgo para planificar la auditoría con base en la información del programa de auditoría y la información documentada proporcionada por el auditado.

Al planificar la auditoría, el líder del equipo auditor debería considerar lo siguiente:

a) La composición del equipo de auditoría y su competencia general.

b) Las técnicas de muestreo apropiadas.

c) Oportunidades para mejorar la efectividad y eficiencia de las actividades de auditoría.

d) Los riesgos para lograr los objetivos de auditoría creados por una planificación de auditoría.
ineficaz
e) Los riesgos para el auditado creados al realizar la auditoría

---

Planificación de Auditoría

Detalles de planificación de auditoría

La planificación de la auditoría debería abordar o hacer referencia a lo siguiente:

a) Los objetivos de la auditoría.

b) El alcance de la auditoría, incluida la identificación de la organización y sus funciones, así como los procesos a auditar.

c) Los criterios de auditoría y cualquier información documentada de referencia.

d) Las ubicaciones (físicas y virtuales), las fechas, el tiempo previsto y la duración de las
actividades de auditoría que se llevarán a cabo, incluidas las reuniones con la administración del auditado.

Planificación de Auditoría

e) La necesidad de que el equipo de auditoría se familiarice con las instalaciones y los procesos del auditado (por ejemplo, realizando un recorrido por la (s) ubicación

(es) física (s), o revisando la tecnología de información y comunicación).
f) Los métodos de auditoría que se utilizarán, incluido el grado en que el muestreo de auditoría es necesario para obtener suficiente evidencia de auditoría.

g) Las funciones y responsabilidades de los miembros del equipo de auditoría, así como guías y observadores o intérpretes.

h) La asignación de recursos apropiados en base a la consideración de los riesgos y oportunidades relacionados con las actividades que se auditarán.

Planificación de Auditoría

La planificación de la auditoría debería tener en cuenta, según corresponda:
- Identificación del (los) representante (s) del auditado para la auditoría
- El lenguaje de trabajo y de informes de la auditoría cuando esto es diferente del lenguaje del auditor o el auditado o ambos.
- Los temas del informe de auditoría
- Arreglos de logística y comunicaciones, incluidos arreglos específicos para las ubicaciones que se auditarán.
- Cualquier acción específica que se tome para abordar los riesgos para alcanzar los objetivos de auditoría y las oportunidades que surjan.
- Cuestiones relacionadas con la confidencialidad y la IA.
- Cualquier acción de seguimiento de una auditoría anterior u otra (s) fuente (es), por ejemplo:
- Lecciones aprendidas, revisiones de proyectos.
- Cualquier actividad de seguimiento de la auditoría planificada.
- Coordinación con otras actividades de auditoría, en caso de una auditoría conjunta.

Planificación de Auditoría

El plan de auditoría debería incluir:

1. Los objetivos de la auditoría.
2. El alcance de la auditoría.
3. Los criterios de la auditoría.
4. Ubicación, las fechas, el horario y la duración incluyendo las reuniones con la dirección del auditado.
5. Las funciones y responsabilidades de los miembros del equipo auditor, así como los guías y observadores.
6. La asignación de los recursos necesarios.
7. La identificación del representante del auditado.
8. El idioma.

El plan de auditoría puede ser revisado y aceptado por el cliente de la auditoría y debería presentarse al auditado.

Recomendación de Taller 1

Se recomienda por parte de la persona instructora realizar:

• Elaborar Plan de Auditoría

Recomendación de Taller 2

Se recomienda por parte de la persona instructora realizar:

• Matriz de Plan de Auditoría

Asignación de Tareas al Equipo Auditor

El líder del equipo auditor, consultando con el equipo auditor, asigna a cada miembro del equipo responsabilidad para:

• Auditar procesos.

• Actividades.

• Funciones.

• Lugares específicos.

Las asignaciones deberían considerar la necesidad de:

• Independencia y competencia de los auditores.

• El uso eficaz de los recursos.

• Diferentes funciones y responsabilidades de los auditores, auditores en formación y expertos técnicos.

Funciones y Responsabilidades de Guías y Observadores

Los guías y observadores pueden acompañar al equipo de auditoría con las aprobaciones del líder del equipo de auditoría, el cliente de auditoría y/o el auditado, de ser necesario.

No deberían influir ni interferir en la realización de la auditoría.

Funciones y Responsabilidades de Guías y Observadores

Para los Guías sus responsabilidades deberían incluir lo siguiente:

a) Ayudar a los auditores a identificar a los individuos para que participen en las entrevistas y confirmen los horarios y las ubicaciones.

b) Organizar el acceso a ubicaciones específicas del auditado.

c) Garantizar que los miembros del equipo de auditoría y los observadores conozcan y respeten las normas relativas a los acuerdos específicos de localización para el acceso, la salud y la seguridad, el medio ambiente, la seguridad, la confidencialidad y otros asuntos, y que se aborden los riesgos.

d) Ser testigo de la auditoría en nombre del auditado, cuando corresponda.

e) Proporcionar aclaraciones o ayudar a recopilar información, cuando sea necesario.

Preparación de los Documentos de Trabajos

Los miembros del equipo auditor deben recopilar y revisar la información pertinente

a las tareas asignadas y preparar los documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría.

(Incluir gráfico)

Posibles Ventajas de las Listas de Verificación

a) Aseguran que nada importante se pase por alto.

b) Ayudan a brindar continuidad a la auditoría.

c) Ayudan a planificar una auditoría eficaz.

d) Ayudan a identificar los aspectos más críticos del sistema.

e) Ayudan a controlar la profundidad, continuidad y ritmo de la auditoría.

f) Registran los hallazgos positivos y negativos.

g) Pueden proporcionar un registro de oportunidades de mejora.
h) Las listas de verificación previamente confeccionadas pueden inhibir a los auditores.

i) Los auditores pueden pasar por alto cuestiones importantes por no estar incluidas en las listas de verificación.

Uso de las Listas de Verificación

a) Considerar las listas de verificación como un ayuda memoria.
b) Evitar sentirse inhibidos por ellas.
c) Escribir prolijamente: la lista de verificación es parte del informe de auditoría.
d) Registrar conclusiones finales.
e) Registrar oportunidades de mejora.
f) Registrar identidades específicas de las muestras examinadas.

Recomendación de Taller 3

Se recomienda por parte de la persona instructora realizar:

• Elaborar una lista de verificación para auditar las cláusulas señaladas por el instructor.

Reunión de Apertura

PROPÓSITO:

a) Confirmar el acuerdo de todos los participantes (por ejemplo, auditado, equipo de auditoría) con el plan de auditoría.

b) Presentar al equipo de auditoría y sus roles.

c) Garantizar que se puedan realizar todas las actividades de auditoría planificadas.

Reunión de Apertura

PUNTOS A CONSIDERAR:

• Los objetivos, el alcance y los criterios de la auditoría

• El plan de auditoría y otros arreglos relevantes con el auditado, como la fecha y hora de la
reunión de cierre, cualquier reunión interina entre el equipo de auditoría y la administración del auditado, y cualquier cambio necesario

• Canales de comunicación formales entre el equipo de auditoría y el auditado.

• El idioma que se utilizará durante la auditoría.

• El auditado debería mantenerse informado del progreso de la auditoría durante la auditoría.

• La disponibilidad de los recursos y las instalaciones que necesita el equipo de auditoría.

• Cuestiones relacionadas con la confidencialidad y la IA.

• Acceso relevante, salud y seguridad, seguridad, emergencia y otros arreglos para el equipo de auditoría.

• Actividades en el sitio que pueden afectar la realización de la auditoría.

Reunión de Apertura

PUNTOS A CONSIDERAR:

La presentación de información sobre los siguientes elementos se debería considerar, según corresponda:

• El método de informar los hallazgos de la auditoría, incluidos los criterios para la calificación, si corresponde.

• Condiciones bajo las cuales puede darse por terminada la auditoría.

• Cómo tratar con posibles hallazgos durante la auditoría.

• Cualquier sistema de retroalimentación del auditado sobre los hallazgos o conclusiones de la auditoría, incluidas las quejas o apelaciones.

Revisión de la Documentación en la Auditoría

La información documentada relevante del auditado debería ser revisada para:

• Determinar la conformidad del sistema, en la medida documentada, con los criterios de auditoría.

• Recopilar información para apoyar las actividades de auditoría.

La revisión se puede combinar con las otras actividades de auditoría y puede continuar a lo largo de la auditoría, siempre que esto no sea perjudicial para la efectividad de la realización de la auditoría.

Si no se puede proporcionar la información documentada adecuada dentro del marco de tiempo dado en el plan de auditoría, el líder del equipo de auditoría debería informar tanto a la (s) persona (s) que gestionan el programa de auditoría como al auditado. Dependiendo de los objetivos y el alcance de la auditoría, se debería tomar una decisión sobre si la auditoría debería continuar o suspenderse hasta que se resuelvan los problemas de información documentada.

Comunicación Durante la Auditoría

Durante la auditoría, puede ser necesario hacer arreglos formales para la comunicación dentro del equipo de auditoría, así como con el auditado, el cliente de auditoría y potencialmente con partes interesadas externas (por ejemplo, reguladores), especialmente cuando los requisitos legales y reglamentarios requieren la notificación obligatoria de incumplimiento.

• El equipo de auditoría debería consultar periódicamente para intercambiar información, evaluar el progreso de la auditoría y reasignar el trabajo entre los miembros del equipo de auditoría, según sea necesario

• Durante la auditoría, el líder del equipo de auditoría debe comunicar periódicamente el avance de la auditoría y cualquier inquietud al auditado

• Cuando los objetivos de la auditoría no sean alcanzables el líder del equipo auditor debería informar de las razones a las partes interesadas para tomar acciones apropiadas

• Las acciones pueden incluir la reconfirmación o la modificación del plan, cambios en los objetivos, alcance o la interrupción de la auditoría

• Los cambios deberían revisarse y aprobarse tanto por el gestor del programa de auditoría como por el auditado.

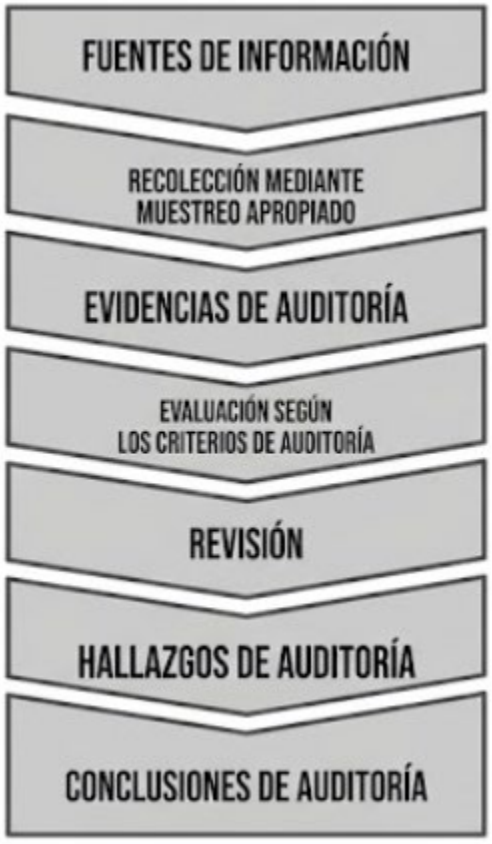
Métodos para Recopilar Información

• Entrevistas
• Observación de actividades o lugares de trabajo.
• Revisión de documentos, incluyendo registros.
• Registros, tales como reportes de ocurrencias de eventos de seguridad, de mediciones de la eficacia de los controles, actas de reunión, informes de auditoría.

• Resúmenes de datos, análisis e indicadores de desempeño de incidentes de seguridad.

• Informes de otras fuentes, por ejemplo, datos de entidades reguladoras.

Métodos para Recopilar Información



Visión general de un proceso típico, desde la recopilación de información hasta llegar a conclusiones de auditoría.

La Entrevistas

a) Las entrevistas deben realizarse con personas de niveles apropiados y funciones que realizan actividades o tareas dentro del alcance de la auditoría.

b) Las entrevistas deben realizarse durante el horario laboral normal y, donde sea práctico, en lugar de trabajo normal de la persona que se está entrevistado.

c) Se debe tratar que la persona que se entrevista esté cómoda antes y durante la entrevista.

d) Se debe explicar la razón para la entrevista y cualquier nota que se tome

e) Se deben resumir y revisar los resultados de la entrevista con la persona entrevistada.

f) Se debe agradecer a las personas entrevistadas por su participación y cooperación.

Preguntas Claves del Auditor

Tipo de Preguntas

- ¿Realizaron auditorías internas?
- ¿Existe una política del Sistema de Gestión?
- ¿El Sistema de Gestión ha sido comunicado?
- ¿Es usted parte del grupo auditor interno?
- ¿El proceso se ejecuta como está documentado?
- ¿En dónde registra la información?
- ¿Cuál procedimiento?
- ¿Conoce la política?
- ¿Cumple la legislación?

Ejecutando la Auditoría

• Haga un muestreo de actividades, no se centre en una.
• Busque evidencia observando lo que ocurre y revisando registros.
• Haga anotaciones completas.
• Escuche las explicaciones del auditado.

• Anote y confirme los hallazgos u observaciones. Si tiene dudas sobre el cumplimiento de un requisito podría hacer algunas preguntas abiertas adicionales.

• Siempre escriba los detalles de lo observado o evidenciado, por ejemplo, debería anotar el procedimiento auditado, los identificadores de los registros, número de órdenes, identificación de lotes, códigos de documentos etc

• Auditoría abierta y amigable resultará en un acuerdo de que el problema existe

• Verifique si la No Conformidad es o no puntual

Realización de Entrevistas

• Sea amigable.
• Haga sentir cómodo al auditado.
• Explicar las razones de la entrevista y de las notas tomadas.
• Iniciar con una descripción de las actividades.
• No realizar preguntas inductivas (Evita preguntas cuya respuesta sea SI o NO).
• Agradecer a los auditados.

Administración del Tiempo

• Realizar primero las actividades más complejas o difíciles.
• Asignar trabajo a los otros auditores.
• Adquirir el hábito de hacerlo de inmediato.

• Conocer curva de cansancio del auditado y auditor.
• Establecer límite de tiempo y cumplirlo.
• Ser creativo.

Manejo de Situaciones Difíciles

• A la reunión de apertura no se presenta el responsable del proceso o actividad auditada.
• En la auditoría se tenía previsto visitar dos instalaciones y no hay disponibles vehículos, ni acompañantes.
• El auditado desvía la pregunta del auditor. Ejemplo: pregunta por la forma como se controlan los documentos y el auditado explica la forma como se controlan los registros, dado que los documentos son un tipo de registro.
• El auditado suministra poca información. Ejemplo: se solicita información sobre los resultados de enero a mayo y solo presenta los resultados del último mes.

• El auditado reformula las preguntas del auditor.

• El auditado cuestiona las preguntas del auditor. Ejemplo: lo que usted pregunta no tiene sentido

• En la reunión de apertura no hay acuerdo con el objeto y alcance de la auditoría.

Resultados de la Auditoría

Hallazgo

• Resultados de la evaluación de la evidencia objetiva recopilada frente al conjunto de políticas, procedimientos o requisitos utilizados como referencia.
• Es registrado en la lista de verificación como respuesta a los cuestionamientos que han sido preparados.

Tipos de Hallazgos

• **No conformidad**: Incumplimiento de un requisito especificado
• **Observación:** Situación que potencialmente puede afectar el sistema de gestión de calidad

---

Incumplimientos Más Comunes

• Documentación no encontrada
• Competencias de recurso humano no evaluada
• Controles implementados inadecuados
• No conformidades por auditorías internas sin cierre eficaz
• Acciones correctivas sin revisión de la dirección
• Deficiencia en metodología de análisis de riesgo
• Incumplimiento de procedimientos

Redacción de las No Conformidades

• **La Evidencia:** Lista de hallazgos, respaldados con evidencias objetivas o atestiguadas por el auditado
• **La Referencia:** Al requisito de la norma y/o manual de calidad o procedimiento. Un requisito a la vez, el que más aplica
• **La Conclusión:** Genérica, breve, precisa y aceptada por el auditado
• **No Conformidad:** Incumplimiento a un requisito de la Norma auditada
• **Observación**: Hallazgo detectado en Auditoría que podría generar una no conformidad si no es tratado
• **Oportunidad de Mejora:** Son situaciones que no representan incumplimiento, pero pueden ser revisadas por la organización, cuando lo estime conveniente para mejorar la eficacia del proceso.

Fórmula de Redacción de No Conformidades

Reporte debe contener como mínimo:

- Una visión general del hallazgo
- Descripción completa y precisa de lo observado
- Ejemplos de la evidencia de auditoría
- Referencia a la cláusula del estándar/documento de la organización
- Explicación de los requisitos de la cláusula/documento
- Las discrepancias deben atribuirse solamente a una cláusula de la norma, la más aplicable
- En ocasiones, la única referencia es la documentación de la organización.

Conclusiones de Auditoría

El equipo auditor debe reunirse antes de la "reunión de cierre" para:

- Revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma
- Acordar conclusiones de auditoría
- Preparar recomendaciones, si así lo especifica el plan de auditoría.

Las conclusiones de auditoría pueden tratar aspectos como:

- Evaluación del grado de cumplimiento con el criterio de auditoría
- Eficacia de la implementación, mantenimiento y mejoras del sistema de gestión
- Capacidad del proceso de revisión por la dirección para asegurar la adecuación, eficacia y mejora sostenida del SGIA.

Informe de Auditoría

Debería contener:

- Objetivos de la auditoría

• Alcance de la auditoría, particularmente la definición de las unidades de la organización o de los procesos auditados y el período de la auditoría
• Documentación de la persona de contacto
• Documentación del auditor líder y otros auditores
• Fechas y ubicaciones donde se desarrollaron las actividades de la auditoría
• Criterio de auditoría
• Declaraciones de auditoría
• Conclusiones de la auditoría

Reunión de Cierre

Es facilitada por el auditor líder. Según corresponda, lo siguiente debería explicarse al auditado en la reunión de clausura:
a) Informar que la evidencia de auditoría recopilada se basó en una muestra de la información disponible y no es necesariamente representativa de la eficacia general de los procesos del auditado

b) El método de informar

c) Cómo debería abordarse la conclusión de la auditoría en función del proceso acordado

d) Posibles consecuencias de no abordar adecuadamente los hallazgos de la auditoría

e) Presentación de los hallazgos y conclusiones de auditoría de tal manera que la gerencia del auditado los comprenda y los reconozca

f) Cualquier actividad posterior a la auditoría relacionada (por ejemplo, implementación y revisión de acciones correctivas, tratamiento de quejas de auditoría, proceso de apelación)

Preparación y Distribución del Informe de Auditoría

El líder del equipo auditor debería informar las conclusiones de la auditoría de acuerdo con el programa de auditoría.

El informe de auditoría debería proporcionar un registro completo, preciso, conciso y claro de la auditoría, e incluir o hacer referencia a lo siguiente:
a) Objetivos de auditoría
b) Alcance de la auditoría, particularmente identificación de la organización (el auditado) y las funciones o procesos auditados

c) Identificación del cliente de auditoría

d) Identificación del equipo de auditoría y los participantes del auditado en la auditoría

---

Preparación y Distribución del Informe de Auditoría

e) Fechas y lugares donde se llevaron a cabo las actividades de auditoría

f) Criterios de auditoría

g) Hallazgos de auditoría y evidencia relacionada

h) Conclusiones de auditoría

i) Una declaración sobre el grado en que se han cumplido los criterios de auditoría

j) Cualquier opinión divergente no resuelta entre el equipo de auditoría y el auditado

k) Las auditorías por naturaleza son un ejercicio de muestreo; como tal, existe el riesgo de que la evidencia de auditoría examinada no sea representativa.

Preparación y Distribución del Informe de Auditoría

El informe de auditoría debería emitirse dentro del tiempo acordado. Si se retrasa, los motivos deberían comunicarse al auditado y a la(s) persona(s) que gestionan el programa de auditoría.

El informe de auditoría debería estar fechado, revisado y aceptado, según corresponda, de conformidad con el programa de auditoría.

El informe de auditoría debería distribuirse a las partes interesadas pertinentes definidas en el programa de auditoría o el plan de auditoría.

Al distribuir el informe de auditoría, se deberían considerar medidas apropiadas para garantizar la confidencialidad.

Preparación y Distribución del Informe de Auditoría

La auditoría se completa cuando se han llevado a cabo todas las actividades de auditoría planificadas, o según se acuerde con el cliente de auditoría (por ejemplo, puede haber una situación inesperada que impida completar la auditoría de acuerdo con el plan de auditoría).

La información documentada relativa a la auditoría debería conservarse o eliminarse por acuerdo entre las personas participantes y de acuerdo con el programa de auditoría y los requisitos aplicables.

A menos que lo exija la ley, el equipo de auditoría y las personas que gestionan el programa de auditoría no deberían divulgar ninguna información obtenida durante la auditoría, o el informe de auditoría, a ninguna otra parte sin la aprobación explícita del cliente de auditoría y, cuando corresponda, la aprobación del auditado.

Las lecciones aprendidas de la auditoría pueden identificar riesgos y oportunidades para el programa de auditoría y el auditado.

Realización de Seguimiento de Auditoría

• **El resultado de la auditoría** puede, dependiendo de los objetivos de la auditoría, indicar la necesidad de correcciones o de acciones correctivas u oportunidades de mejora. Tales acciones generalmente son decididas y llevadas a cabo por el auditado dentro de un plazo acordado. Según corresponda, el auditado debería mantener informadas a las personas que gestionan el programa de auditoría y/o al equipo de auditoría sobre el estado de estas acciones.

• **La finalización y efectividad de estas acciones debería ser verificada.** Esta verificación puede ser parte de una auditoría posterior. Los resultados se deberían informar a la persona que gestiona el programa de auditoría y se informa al cliente de auditoría para su revisión por la dirección.

Las Auditorías de Seguimiento

Responsabilidades del auditor:

• Acordar la fecha de la auditoría de seguimiento
• Desarrollar la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas

• Presentar e informar los resultados de la auditoría de seguimiento

• Evaluar la eficacia de las acciones correctivas y preventivas implantadas

---

Recomendación de Taller 4

• Según el formato, se recomienda por parte de la persona instructora realizar el informe de auditoría a sus estudiantes.

Conclusiones

La Norma ISO 42001 puede ser implementada en cualquier tipo de organización pues proporciona una metodología para implementar un Sistema para la Gestión de la Seguridad de la Información, permitiendo también que una empresa sea certificada según el cumplimiento de esta norma, donde su eje central es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa.

Contenido para Comunidad exclusiva

Bienvenida a I42001IA™: Auditar un SGIA con evidencia objetiva

En organizaciones que usan IA para decisiones críticas, auditar el SGIA exige evidencia verificable, no percepciones ni "buenas intenciones".

Sabías que: En auditoría (ISO 19011), la evidencia debe ser **objetiva y verificable**; entrevistas sin registros suelen ser insuficientes para sustentar conformidad.

Autoevaluación: ¿Qué evidencia "mínima" pedirías si alguien afirma: "sí hacemos evaluación de impacto" pero no muestra registros?

Propósito de esta guía de autoestudio (recomendatoria, no obligatoria)

Esta guía organiza la preparación del examen priorizando criterios, evidencia y eficacia del SGIA; es apoyo voluntario, no requisito del examen.

Sabías que: Un buen material de autoestudio no reemplaza la norma: ayuda a **interpretar requisitos** y a entrenar el "ojo auditor" para detectar las brechas con evidencia.

Autoevaluación: ¿Tu estrategia actual de estudio se centra más en memorizar cláusulas o en reconocer qué evidencia demuestra conformidad?

Qué valida I42001IA™ frente a Foundation

I42001IA™ evalúa competencia para planificar y ejecutar auditorías internas del SGIA, determinando conformidad y eficacia con evidencia objetiva.

Sabías qué: Foundation se enfoca en comprensión estructural; Internal Auditor exige interpretar situaciones y **sustentar hallazgos** con criterios y evidencia.

Autoevaluación: ¿Qué cambia en tu rol cuando pasas de "entender la norma" a "auditar su cumplimiento"?

Enfoque del rol auditor: conformidad + eficacia + mejora

Auditar el SGIA no es "revisar documentos": es verificar si el sistema logra resultados previstos y mejora, mediante controles y gestión de riesgos.

Sabías que: En auditoría de sistemas de gestión, el juicio no es solo "cumple/no cumple"; también evalúa la **eficacia** (si el control funciona en operación).

Autoevaluación: Piensa en un control de IA (p.ej., monitoreo de sesgo). ¿Qué evidencias mostrarían eficacia, no solo existencia?

El triángulo auditor: Criterios – Evidencia – Conclusión

Una conclusión de auditoría se sostiene cuando el criterio es claro, la evidencia es suficiente y apropiada, y la conclusión es trazable.

Sabías que: Un error típico es confundir "alcance" con "criterios": el alcance delimita *qué* auditas; los criterios definen *contra qué* comparas.

Autoevaluación: Si auditas “evaluación de riesgos de IA”, ¿cuáles serían tus criterios (norma/procedimiento) y cuál sería el alcance (procesos/período/sistemas)?

Mapa mental ISO/IEC 42001 para auditoría (HLS y trazabilidad)

Para auditar con precisión, ubica cada hallazgo en la cláusula correcta (4–10) y conecta PDCA con riesgos, controles, evaluación y mejora.

Sabías que: La estructura armonizada (HLS) facilita integrar auditorías del SGIA con otros sistemas (calidad/seguridad), reutilizando prácticas como 9.2 y 9.3.

Autoevaluación: Si encuentras “no hay auditoría interna del SGIA”, ¿en qué capítulo cae y qué evidencia buscarías del programa/plan?

Preparación tipo examen: pensar como auditor, responder como norma

Las preguntas suelen medir tu capacidad de identificar el requisito aplicable y el tipo de evidencia que demostraría conformidad o no conformidad.

Sabías que: En preguntas situacionales, el distractor frecuente es “una buena práctica” que no está sustentada por evidencia documentada o método definido.

Autoevaluación: ¿Qué te haría descartar una opción que suena “correcta” pero no menciona evidencia, registros o criterios?

Tipos de evidencia y errores comunes en auditorías de IA

En IA, la evidencia suele combinar registros de ciclo de vida, decisiones de riesgo, SoA, métricas y trazas operativas; “solo verbal” es débil.

Sabías que: En sistemas algorítmicos, la evidencia robusta suele requerir **triangulación**: documento + entrevista + observación/registro del sistema.

Autoevaluación: ¿Qué 3 fuentes de evidencia triangularías para verificar que el monitoreo en producción opera como se define?

Footer: Licensed under CC BY 4.0.

Cómo usar esta guía: estudio por módulos + práctica de juicio auditor

Avanza por módulos y practica: (1) ubicar cláusula, (2) definir criterio, (3) pedir evidencia, (4) redactar conclusión defendible.

Sabías que: El objetivo no es “cazar errores”, sino aportar valor: un hallazgo bien formulado ayuda a mejorar el SGIA y reducir riesgos.

Autoevaluación: Cuando detectas una brecha, ¿sabes formularla como “criterio–condición–evidencia” sin opiniones personales?

Footer: Licensed under CC BY 4.0.

Cierre del Módulo 0: punto de partida del auditor del SGIA

Con esta base, iniciarás el módulo 1 entendiendo contexto, alcance y terminología para auditar IA con precisión y consistencia.

Sabías que: Un auditor efectivo empieza por el contexto: sin comprender alcance y partes interesadas, el muestreo y los hallazgos pierden relevancia.

Autoevaluación: ¿Qué pregunta harías primero para validar si el alcance del SGIA es auditable y no una declaración ambigua?

Panorama del Módulo 1: de “leer” la norma a “auditarla”

Para auditar un SGIA necesitas ubicar rápidamente *qué* exige ISO/IEC 42001 en las Cláusulas 1–4 y *qué* términos usar sin ambigüedad (IA, sistema de IA, ciclo de vida, impacto, partes interesadas). Este módulo te entrena a convertir conceptos en preguntas de auditoría y evidencia verificable.

Sabías que: En auditoría, dominar terminología reduce “hallazgos discutibles”: si el término es claro, el criterio también.

Autoevaluación: ¿Qué término de IA te genera más ambigüedad al auditar: “modelo”, “sistema de IA” o “uso de IA”?

Cláusula 1: Objeto y campo de aplicación (qué cubre ISO/IEC 42001)

La Cláusula 1 explica que ISO/IEC 42001 define requisitos para establecer, implementar, mantener y mejorar un SGIA. Como auditor, aquí defines el “marco del juego”: auditas el **sistema de gestión**, no la “calidad del algoritmo” en sí, y verificas que la organización gestione IA de forma controlada y trazable.

Sabías que: En una auditoría se puede revisar el desempeño del sistema de IA como evidencia, pero el criterio principal es el requisito del SGIA.

Autoevaluación: Si la empresa presume "alta precisión del modelo", ¿qué preguntarías para conectar eso con requisitos del SGIA?

Cláusula 2: Referencias normativas (cómo afectan criterios de auditoría)

Las referencias normativas indican documentos esenciales vinculados a la norma. En auditoría, esto impacta tus **criterios**: si un requisito remite a definiciones u orientación normativa, debes asegurar que la organización no contradiga esas referencias en su sistema (procedimientos, políticas, evaluaciones).

Sabías que: Un error frecuente es usar "mejores prácticas" como criterio; el criterio debe provenir de norma, requisitos legales o reglas internas aplicables.

Autoevaluación: ¿Qué diferencia hay entre "referencia normativa" y "bibliografía recomendada" al definir criterios?

Cláusula 3: Términos y definiciones (la base del juicio auditor)

La Cláusula 3 fija el lenguaje común. Para auditoría, lo crítico es evitar confusiones: *SGIA* no es el sistema de IA; *control* no es un "objetivo"; *riesgo* no es "impacto". Con definiciones claras, puedes pedir evidencia correcta, evaluar conformidad y redactar hallazgos defendibles.

Sabías que: Muchas no conformidades "nacen" por definiciones internas inconsistentes (p.ej., "incidente" vs "evento").

Autoevaluación: ¿Qué término deberías exigir que esté definido en el SGIA antes de auditar controles: “riesgo residual” o “innovación”?

SGIA vs Sistema de IA: la confusión más costosa en auditoría

Un **SGIA** es el marco de gestión (políticas, procesos, roles, medición, mejora). Un **sistema de IA** es la solución que produce resultados (modelo + datos + componentes + operación). En auditoría, si confundes ambos, terminas evaluando “tecnología” sin criterio de gestión o revisando “documentos” sin evidencias operativas.

Sabías que: Un mismo SGIA puede cubrir varios sistemas de IA; y un sistema de IA puede cambiar sin que el SGIA cambie… si el cambio está controlado.

Autoevaluación: ¿Qué evidencia te confirma que existe SGIA más allá de que exista un modelo en producción?

Ecosistema de IA: roles típicos que influyen en evidencias

El ecosistema de IA suele incluir: dueños de proceso, data owners, desarrollo/ML, operaciones, seguridad, legal/compliance, proveedores y usuarios. Como auditor, mapeas quién decide, quién ejecuta y quién aprueba, porque de ahí salen evidencias: aprobaciones, registros de validación, monitoreo, incidencias, cambios y comunicaciones.

Sabías que: Si no hay “dueño” claro del sistema de IA, la evidencia se dispersa y la trazabilidad se rompe.

Autoevaluación: En tu organización, ¿quién "firma" la aceptación de riesgo residual de un sistema de IA?

Ciclo de vida del sistema de IA: qué se audita en cada fase

El ciclo de vida abarca diseño, desarrollo, validación, despliegue, operación, cambios y retiro. En auditoría, no revisas solo "el inicio"; verificas controles y evidencias por fase: criterios de aceptación, pruebas, autorizaciones, monitoreo de deriva, incidentes y decisiones de retiro. La clave es trazabilidad end-to-end.

Sabías que: Muchos fallos aparecen en operación (monitoreo/deriva), no en entrenamiento; por eso el ciclo de vida es evidencia continua.

Autoevaluación: ¿Qué evidencia pedirías para demostrar que un cambio de modelo fue controlado y aprobado?

Evaluación de impacto del sistema de IA: cuándo y cómo se vuelve "auditable"

La evaluación de impacto es un proceso formal para identificar y abordar efectos en personas o grupos. Para auditoría, lo "auditable" es la trazabilidad: método usado, alcance, resultados, decisiones y seguimiento. No basta con un documento; debe conectarse con riesgos, controles y acciones (y actualizarse ante cambios significativos).

Sabías que: Una evaluación de impacto "sin dueño" ni fecha de revisión suele convertirse en evidencia débil ante auditoría.

Autoevaluación: ¿Qué indicio te muestra que la evaluación de impacto influye realmente en el tratamiento del riesgo?

Cláusula 4.1: Contexto interno y externo (punto de partida del alcance)

La organización debe entender factores internos y externos relevantes para el SGIA: regulación, mercado, tecnología, cultura, capacidades y estrategia. Como auditor, buscas evidencia de un análisis real (no genérico) y verificas que el contexto se refleje en alcance, riesgos, objetivos y controles. Contexto mal definido = auditoría sin foco.

Sabías que: Un contexto desactualizado suele explicar por qué el SGIA "cumple en papel" pero falla en operación (cambió la realidad, no el sistema).

Autoevaluación: ¿Qué documento/registro te indicaría que el contexto se revisa cuando cambia la regulación?

Cláusula 4.2: Partes interesadas y requisitos (declarar vs demostrar)

Identificar partes interesadas implica definir quién puede afectar o ser afectado por IA (clientes, usuarios, reguladores, proveedores, empleados). En auditoría, verificas dos cosas: que estén identificadas y que sus requisitos aplicables se traduzcan en controles, comunicación y monitoreo. No es "listar"; es incorporar.

Sabías que: Un requisito de parte interesada puede ser legal, contractual o reputacional; si es aplicable, debe tratarse en el SGIA.

Autoevaluación: ¿Cómo confirmarías con evidencia que un requisito regulatorio fue incorporado al SGIA?

Cláusula 4.3: Alcance del SGIA (límites, interfaces y exclusiones justificadas)

El alcance define límites y aplicabilidad del SGIA: procesos, unidades, ubicaciones, sistemas de IA, interfaces con terceros y exclusiones justificadas. Como auditor, evalúas si el alcance es claro, consistente con el contexto y verificable. Un alcance ambiguo impide muestreo efectivo y permite "evadir" requisitos críticos.

Sabías que: Alcance "demasiado amplio" sin recursos genera SGIA inoperable; alcance "demasiado estrecho" sin justificación genera brechas y riesgos ocultos.

Autoevaluación: ¿Qué pregunta harías para detectar una exclusión "conveniente" pero no justificada?

Cláusula 4.4: Establecer el SGIA (procesos e interacciones)

ISO/IEC 42001 exige establecer e implementar procesos del SGIA y sus interacciones. En auditoría, esto se traduce en verificar: mapa de procesos, responsabilidades, entradas/salidas, controles integrados y evidencias de operación. El SGIA debe funcionar como sistema, no como "colección de documentos".

Sabías que: Un buen mapa de procesos permite auditar por trazabilidad: de riesgo → control → evidencia → resultado, sin perderse en papeles.

Autoevaluación: ¿Qué evidencia usarías para demostrar que un proceso del SGIA opera "en intervalos planificados"?

Caso Aplicado: Contexto y Alcance Deficiente en una Fintech

Una Fintech usa IA para scoring crediticio automatizado. En auditoría del SGIA se detecta que el análisis de contexto no considera regulación financiera vigente, no identifica reguladores ni clientes como partes interesadas, y el alcance excluye el sistema crítico alegando que es SaaS externo. El SGIA no cubre el proceso más sensible del negocio.

Sabías que:
Excluir un sistema crítico por ser "externo" no elimina la responsabilidad organizacional. ISO/IEC 42001 exige gestionar IA según el rol y el impacto, incluso si el proveedor desarrolla la tecnología.

Autoevaluación:
Si fueras auditor, ¿formularías este hallazgo contra 4.1 (Contexto), 4.2 (Partes interesadas) o 4.3 (Alcance)? ¿Por qué?

Respuesta orientativa para validación del candidato:
El hallazgo puede estructurarse principalmente contra **4.3 (Alcance)**, porque el SGIA excluye injustificadamente el sistema crítico. No obstante, la causa raíz se relaciona también con **4.1 (Contexto)** por no considerar regulación relevante y con **4.2 (Partes interesadas)** por omitir reguladores y clientes afectados. Un auditor competente puede formular un hallazgo principal en 4.3 y referenciar debilidades en 4.1 y 4.2 como contribuyentes sistémicos.

Caso Resuelto – Matriz Recomendada de Evidencia (Cláusulas 4.1–4.3)

Tras la auditoría, la organización actualiza contexto, partes interesadas y alcance.
A continuación, se muestra una **plantilla recomendada** para estructurar evidencia auditables en SGIA.

Matriz Recomendada – Contexto y Alcance del SGIA

(Modelo sugerido para fines formativos)

Elemento Cláusula	Evidencia Documentada	Responsable	Fecha Revisión	Trazabilidad
4.1 Contexto externo	Identificación regulación financiera X y Ley protección datos Y	CRO	15/02/2026	Vinculado a matriz de riesgos IA
4.1 Contexto interno	Apetito de riesgo aprobado por Dirección	CEO	10/02/2026	Referenciado en política IA
4.2 Partes interesadas	Regulador financiero, clientes evaluados, proveedor SaaS	Compliance	18/02/2026	Vinculado a requisitos legales
4.3 Alcance SGIA	Incluye sistema ScoringAI v3.2 y monitoreo operacional	Dirección	20/02/2026	Conectado a SoA y evaluación de riesgos

---

Nota pedagógica:
Esta matriz es una **recomendación formativa** para fortalecer trazabilidad y facilitar auditorías internas. No es un formato obligatorio de la norma.

Sabías que:
Una buena evidencia debe permitir al auditor responder: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Cómo se vincula con el riesgo?

Autoevaluación:
¿Agregarías una columna adicional (por ejemplo, "Evidencia verificada en auditoría") para reforzar la trazabilidad?

Cierre del Módulo 1: checklist mínimo para iniciar una auditoría del SGIA

Antes de entrar a cláusulas 5–10, un auditor IA debería confirmar: (1) terminología consistente, (2) contexto actualizado, (3) partes interesadas y requisitos aplicables, (4) alcance definido y justificable, (5) procesos del SGIA descritos e implementados. Esto habilita muestreo, criterios claros y evidencia objetiva.

Sabías que: Muchos programas de auditoría fallan por empezar "en controles" sin validar primero alcance y contexto.

Autoevaluación: Si solo pudieras verificar 3 elementos antes de auditar, ¿cuáles elegirías y por qué?

MÓDULO 2

Liderazgo y Planificación (Cláusulas 5–6 ISO/IEC 42001)

Enfoque: Dom. C (C8, C9) + ISO/IEC 23894
Objetivo auditor: verificar coherencia política–objetivos–riesgo–SoA y trazabilidad de decisiones

---

Transición: De Contexto a Dirección Estratégica

En el Módulo 1 analizaste el contexto, partes interesadas y alcance del SGIA. Ahora avanzamos hacia el núcleo estratégico: liderazgo, política, objetivos y gestión de riesgos. Como auditor interno, tu enfoque cambia: ya no solo verificas definiciones formales, sino la coherencia entre decisiones directivas y su implementación real en el sistema.

Sabías que:
Muchas no conformidades estructurales se originan en fallas de liderazgo y planificación, no en controles operativos.

Autoevaluación:
¿Estás preparado para auditar decisiones estratégicas y no solo documentos?

2.1 Liderazgo en el SGIA

Liderazgo y Compromiso (Cláusula 5.1)

La alta dirección debe demostrar liderazgo activo e integración del SGIA en la estrategia organizacional. El auditor busca evidencia objetiva de participación real: asignación de recursos, revisión periódica del desempeño, aprobación de decisiones críticas y gestión de riesgos asociados a sistemas IA.

Sabías que:
Delegar completamente el SGIA en áreas técnicas puede indicar incumplimiento de liderazgo.

Autoevaluación:
¿Qué evidencia concreta solicitarías para demostrar compromiso real?

Gobierno y Rendición de Cuentas

El SGIA requiere roles, responsabilidades y autoridades claramente definidas. El auditor evalúa si existe estructura de gobierno que permita aprobar sistemas IA, gestionar riesgos e intervenir ante incidentes algorítmicos con responsabilidad definida.

Sabías que:
La ambigüedad en roles genera vacíos críticos frente a impactos regulatorios o éticos.

Autoevaluación:
¿La organización puede demostrar quién asume la responsabilidad final ante un incidente IA?

Integración del SGIA en la Estrategia

El SGIA no debe operar como sistema aislado. El auditor analiza si está integrado con gestión de riesgos corporativos, cumplimiento normativo y estrategia digital.

Sabías que:
Un SGIA desconectado produce objetivos formales sin impacto real.

Autoevaluación:
¿Los objetivos de IA están alineados con el plan estratégico institucional?

2.2 Política de IA (C8)

Política de IA: Requisitos Auditables (Cláusula 5.2)

La política debe ser apropiada al propósito organizacional, incluir compromiso con mejora continua y gestión de riesgos IA. El auditor verifica aprobación formal, comunicación interna y disponibilidad documentada.

Sabías que:
Una política sin evidencia de comunicación efectiva es una debilidad del sistema.

Autoevaluación:
¿Cómo verificarías que fue comunicada y comprendida?

Coherencia Política–Objetivos–Riesgos

La política debe servir como marco para establecer objetivos medibles. El auditor analiza trazabilidad entre compromisos declarados y métricas concretas asociadas a riesgos IA.

Sabías que:
Declarar "IA ética" sin indicadores es una inconsistencia auditada frecuentemente.

Autoevaluación:
¿Existe indicador asociado a cada compromiso estratégico?

Vigencia y Revisión de la Política

La política debe mantenerse actualizada según cambios regulatorios o tecnológicos. El auditor revisa fecha de actualización y evidencia de revisión periódica.

Sabías que:
Una política desactualizada puede invalidar coherencia del SGIA completo.

Autoevaluación:
¿Refleja cambios recientes en regulación o contexto IA?

Comunicación y Concienciación

No basta con publicar la política. El auditor puede utilizar entrevistas, encuestas o revisión de capacitaciones para evaluar comprensión organizacional.

Sabías que:
ISO 19011 enfatiza el enfoque basado en evidencia y entrevistas como método válido de auditoría.

Autoevaluación:
¿Cómo confirmarías que el equipo técnico entiende los compromisos de la política?

Caso Auditor: Política Desconectada

La política menciona "transparencia algorítmica", pero no existen lineamientos ni métricas asociadas. El auditor debe evaluar coherencia sistémica y posible no conformidad.

Sabías que:
Este análisis corresponde a la competencia C8 del esquema I42001IA™.

Autoevaluación:
¿Formularías hallazgo por incoherencia o incumplimiento parcial?

◇ 2.3 Objetivos de IA

Objetivos Medibles (Cláusula 6.2)

Los objetivos deben ser coherentes con la política, medibles y monitoreables. El auditor verifica indicadores, responsables y plazos definidos.

Sabías que:
Un objetivo ambiguo impide evaluar eficacia del SGIA.

Autoevaluación:
¿El objetivo permite determinar claramente cumplimiento o incumplimiento?

Planificación para Lograr Objetivos

Debe existir planificación documentada para alcanzar los objetivos. El auditor evalúa recursos asignados y seguimiento.

Sabías que:
Un objetivo sin plan asociado representa debilidad estructural.

Autoevaluación:
¿Qué evidencia solicitarías para validar implementación real?

Coherencia Estratégica

Los objetivos deben considerar riesgos y oportunidades identificados.

Sabías que:
La falta de alineación puede generar controles innecesarios o riesgos sin tratamiento.

Autoevaluación:
¿Los objetivos responden a riesgos priorizados?

2.4 Planificación Basada en Riesgos

Enfoque Basado en Riesgos (Cláusula 6.1)

La organización debe determinar riesgos y oportunidades que afecten al SGIA. El auditor evalúa metodología aplicada y consistencia.

Sabías que:
El enfoque basado en riesgos es principio clave también en ISO 19011.

Autoevaluación:
¿El método es repetible y documentado?

Riesgos y Oportunidades en IA

En IA, oportunidades mal gestionadas pueden convertirse en riesgos reputacionales o regulatorios.

Autoevaluación:
¿La organización distingue claramente ambos conceptos?

◇ 2.5 Evaluación de Riesgos IA (ISO 23894)

Marco ISO 23894 como Referencia Técnica

Aunque no es certificable en este esquema, ISO 23894 aporta guía metodológica para evaluar riesgos específicos de IA.

Autoevaluación:
¿La metodología considera ciclo de vida completo del sistema IA?

Entradas Auditables de la Evaluación de Riesgos

Contexto, partes interesadas, tipo de sistema IA, datos utilizados y posibles impactos.

Autoevaluación:
¿Las fuentes de información están documentadas?

Salidas Auditables

Nivel de riesgo, criterios de aceptación y decisiones de tratamiento documentadas.

Autoevaluación:
¿Existe aprobación formal del riesgo residual?

Trazabilidad Riesgo–Decisión

Cada riesgo identificado debe tener decisión documentada y responsable asignado.

Autoevaluación:
¿Puedes reconstruir el razonamiento detrás de una aceptación de riesgo?

2.6 Evaluación de Impacto IA

¿Cuándo Aplica la Evaluación de Impacto?

Aplica cuando sistemas IA pueden afectar derechos o intereses de personas.

Autoevaluación:
¿La organización definió criterios de activación?

Evidencia Documentada de Impacto

El auditor revisa análisis formal, participación interdisciplinaria y medidas de mitigación.

Autoevaluación:
¿Existe registro formal aprobado?

◇ 2.7 Tratamiento del Riesgo y SoA (C9)

Tratamiento del Riesgo

La organización selecciona controles para modificar riesgos identificados. El auditor evalúa coherencia entre nivel de riesgo y controles implementados.

Autoevaluación:
¿Los controles reducen efectivamente el riesgo?

Introducción a la Declaración de Aplicabilidad (SoA)

La SoA documenta controles necesarios y justificación de inclusión o exclusión. Es pieza clave de trazabilidad estratégica.

Autoevaluación:
¿Puede justificarse formalmente cada exclusión?

◇ CIERRE DEL MÓDULO 2 – CASO INTEGRADOR

Caso Integrador: Política y Riesgo Desalineados

Empresa de salud implementa IA para priorización de pacientes.

Hallazgos:

- Política declara “equidad algorítmica”.
- No existen métricas de sesgo.
- Evaluación de riesgos omite impacto en grupos vulnerables.
- No hay evaluación formal de impacto.
- SoA excluye supervisión humana por “confianza en proveedor”.

Autoevaluación:
¿Dónde formularías el hallazgo principal?

Resolución Modelo Auditor

Cláusulas afectadas:

- 5.2 Política (incoherencia).
- 6.1 Identificación de riesgos (omisión impacto).
- 6.1.3 Tratamiento y SoA (exclusión injustificada).

Naturaleza: Hallazgo sistémico por ruptura en trazabilidad:

Política → Objetivo → Riesgo → Control → Justificación SoA

Clasificación posible: No Conformidad Mayor.

Autoevaluación:
¿Podrías defender esta clasificación ante la dirección?

Plantilla Recomendada – Matriz de Trazabilidad Estratégica

Elemento	Evidencia Esperada	Estado	Observación Auditor	Impacto
Política	KPI de equidad	No	No definido	Alto
Objetivos	Indicador sesgo	No	No existe	Alto
Riesgos	Impacto grupos vulnerables	No	Riesgo omitido	Crítico
Impacto	Documento formal	No	No realizado	Crítico
SoA	Justificación exclusión	Débil	Basada en proveedor	Alto

Nota: Plantilla recomendada para práctica formativa. No obligatoria por la norma.

Autoevaluación Final:

¿Cómo presentarías este hallazgo para fomentar mejora y no confrontación?

MÓDULO 3

Soporte y Operación (Cláusulas 7–8 ISO/IEC 42001)

Enfoque: Dom. C – C10 y C11
Objetivo auditor: determinar aplicabilidad de controles y evaluar su diseño, implementación y eficacia con evidencia objetiva

---

Transición: De la Planificación Estratégica al Control Real

En el Módulo 2 analizaste cómo la alta dirección define política, objetivos y riesgos. Sin embargo, un SGIA no se valida por la calidad de su planificación, sino por la solidez de su ejecución. En este módulo pasarás del "deber ser" estratégico al "cómo se ejecuta realmente". El foco del auditor interno cambia: ahora debe evaluar competencia, documentación, controles operativos y eficacia demostrable en condiciones reales.

El juicio ya no se basa en declaraciones, sino en evidencia verificable.

Sabías que:
La mayoría de no conformidades mayores en sistemas de gestión surgen en la fase de operación, no en planificación.

Autoevaluación:
¿Estás preparado para cuestionar si el control funciona, no solo si existe?

3.1 Soporte (Cláusula 7)

Competencia como Condición de Control (7.2)

La competencia no es un requisito administrativo, sino un control preventivo. En un SGIA, decisiones sobre datos, modelos, supervisión y monitoreo impactan riesgos éticos, regulatorios y reputacionales. El auditor debe evaluar si las personas que influyen en estos procesos poseen conocimiento demostrable en gestión de riesgos IA, ciclo de vida del sistema y controles aplicables.

La evidencia no se limita a certificados; debe incluir aplicación práctica, experiencia verificable y resultados consistentes.

Sabías que:
Un modelo técnicamente correcto puede generar riesgo sistémico si quienes lo gestionan no comprenden sus implicaciones regulatorias.

Autoevaluación:
¿Qué tipo de evidencia demostraría competencia aplicada y no solo formación recibida?

Concienciación como Mecanismo de Mitigación (7.3)

La concienciación garantiza que el personal entienda la política, los riesgos y las consecuencias de incumplimiento. El auditor debe ir más allá del registro de capacitaciones y evaluar comprensión real mediante entrevistas estructuradas, revisión de decisiones tomadas y coherencia entre discurso y práctica operativa.

Un SGIA puede fallar no por ausencia de controles, sino por desconocimiento de su propósito.

Sabías que:
En auditoría basada en evidencia, la entrevista es válida cuando se triangula con documentación y registros.

Autoevaluación:
Si entrevistas a un desarrollador, ¿podría explicar cómo su trabajo impacta los riesgos del SGIA?

Comunicación Efectiva y Gestión de Incidentes (7.4)

La comunicación en el SGIA no es solo informativa, sino estratégica. Debe definir qué se comunica, cuándo, a quién y bajo qué condiciones. El auditor evalúa protocolos ante incidentes IA, notificación a partes interesadas y consistencia entre canales internos y externos.

Una falla comunicacional puede amplificar el impacto de un riesgo ya materializado.

Sabías que:
La ausencia de protocolo formal de comunicación ante incidentes puede ser hallazgo mayor si el sistema IA afecta derechos.

Autoevaluación:
¿Existe evidencia de simulaciones o pruebas del protocolo de comunicación?

Información Documentada como Soporte del Juicio (7.5)

La documentación del SGIA debe ser controlada, actualizada y accesible. El auditor verifica control de versiones, autorizaciones formales y coherencia entre documentos estratégicos y operativos.

Documento sin control equivale a pérdida de confiabilidad del sistema.

La documentación debe permitir reconstruir decisiones, tratamientos de riesgo y cambios implementados.

Sabías que:
Una SoA desactualizada invalida la trazabilidad riesgo–control.

Autoevaluación:
¿Puedes identificar fácilmente la versión vigente de cada documento crítico?

3.2 Operación (Cláusula 8)

Planificación y Control Operacional (8.1)

La operación del SGIA exige que los procesos estén planificados y controlados conforme a los riesgos identificados. El auditor analiza si existen procedimientos claros, responsabilidades asignadas y registros de ejecución.

El control operacional debe demostrar consistencia en condiciones normales y ante escenarios de excepción.

No basta con diseñar un control; debe ejecutarse sistemáticamente.

Sabías que:
Un procedimiento no aplicado constituye falla operacional, no documental.

Autoevaluación:
¿El proceso operativo produce evidencia repetible y verificable?

3.2 Operación (Cláusula 8)

Planificación y Control Operacional (8.1)

La Cláusula 8 exige que la organización planifique, implemente y controle los procesos necesarios para cumplir requisitos del SGIA y tratar riesgos identificados. Desde la perspectiva del auditor interno, esto implica verificar que los controles seleccionados en la SoA estén efectivamente integrados en los procesos operativos, con responsables definidos, criterios de ejecución y evidencia trazable.

No se audita intención, se audita ejecución verificable.

Sabías que:
Un control documentado pero no integrado al flujo operativo real constituye falla de implementación, no de diseño.

Autoevaluación:
¿Puedes demostrar que el control forma parte del proceso diario y no es una actividad aislada?

Gestión de Cambios en Sistemas de IA

Los sistemas de IA evolucionan: actualización de modelos, ajustes de datos, cambios en proveedores o parámetros. La auditoría debe evaluar si existe procedimiento formal de gestión de cambios que incluya análisis de impacto, aprobación previa, actualización de evaluación de riesgos y revisión de la SoA cuando corresponda.

Un cambio no controlado puede invalidar el tratamiento de riesgos previamente aprobado.

Sabías que:
Muchos incidentes algorítmicos se originan en cambios no evaluados adecuadamente.

Autoevaluación:
¿La organización puede demostrar análisis de impacto antes de cada actualización significativa del modelo?

Procesos Externalizados y Responsabilidad Residual

ISO/IEC 42001 no permite transferir responsabilidad del SGIA a proveedores externos. Si el sistema IA es SaaS o tercerizado, la organización debe demostrar evaluación, selección, monitoreo y control continuo del proveedor.

El auditor debe revisar contratos, cláusulas de control, SLAs y evidencia de seguimiento periódico.

La externalización no elimina la obligación de control.

Sabías que:
Una exclusión en la SoA basada únicamente en “confianza en proveedor” es técnicamente débil.

Autoevaluación:
¿Existe evidencia de supervisión periódica y evaluación de desempeño del proveedor IA?

Control Operacional y Riesgo Residual

El tratamiento del riesgo solo es eficaz si el riesgo residual se reduce a niveles aceptables definidos por la organización. El auditor debe verificar que existan criterios documentados de aceptación y evidencia posterior a la implementación del control que confirme reducción efectiva del riesgo.

Sin medición posterior, no existe confirmación de eficacia.

Sabías que:
Aceptar riesgo residual sin análisis documentado puede derivar en no conformidad mayor.

Autoevaluación:
¿Puedes identificar la diferencia entre “riesgo mitigado” y “riesgo aceptado”?

◇ 3.3 Anexo A – Controles de Referencia

Naturaleza del Anexo A

El Anexo A de ISO/IEC 42001 presenta controles de referencia organizados para apoyar el tratamiento de riesgos IA. No es un checklist obligatorio ni exige implementación total. La auditoría debe evaluar la lógica de selección, no la cantidad de controles adoptados.

El criterio clave es pertinencia y coherencia con el contexto y riesgos.

Sabías que:
Aplicar todos los controles sin análisis puede indicar falta de madurez metodológica.

Autoevaluación:
¿La organización puede explicar por qué cada control fue seleccionado?

Controles vs Objetivos de Control

Un control es una medida específica que modifica un riesgo. El objetivo de control es el resultado esperado que el control pretende lograr. El auditor debe distinguir claramente ambos conceptos para evaluar diseño y eficacia.

Confundir objetivo con control puede generar debilidad conceptual en la SoA.

Sabías que:
Un control sin objetivo definido impide evaluar eficacia real.

Autoevaluación:
¿Puedes identificar el objetivo detrás de cada control implementado?

Coherencia entre Anexo A y Matriz de Riesgos

La auditoría debe verificar que cada control seleccionado esté vinculado a un riesgo identificado previamente. La trazabilidad riesgo → control → evidencia es eje central del Dominio C del examen.

Sin trazabilidad documentada, el sistema pierde integridad lógica.

Sabías que:
La falta de correspondencia entre riesgo alto y ausencia de control es hallazgo crítico.

Autoevaluación:
¿Cada riesgo significativo tiene control asignado?

3.4 SoA en Auditoría (C10)

Contenido Técnico Mínimo de la SoA

La Declaración de Aplicabilidad debe incluir: lista de controles seleccionados, justificación de inclusión/exclusión, referencia al riesgo asociado y estado de implementación. El auditor debe poder reconstruir el razonamiento estratégico detrás de cada decisión.

La SoA es documento estratégico, no inventario administrativo.

Sabías que:
Una SoA sin vínculo explícito a la matriz de riesgos debilita la defensa técnica del SGIA.

Autoevaluación:
¿La SoA permite entender por qué un control fue descartado?

Determinación de Aplicabilidad (C10)

La aplicabilidad de controles debe basarse en análisis objetivo del contexto, criticidad del sistema IA y nivel de riesgo identificado. El auditor evalúa si la metodología de selección es consistente, documentada y repetible.

La aplicabilidad no puede fundamentarse en conveniencia operativa.

Sabías que:
La exclusión injustificada de controles de supervisión humana es frecuente en auditorías IA.

Autoevaluación:
¿La metodología de selección está formalmente definida?

Muestreo Basado en Riesgo para Evaluar Aplicabilidad

El auditor interno puede priorizar revisión de controles asociados a riesgos altos, sistemas críticos o impactos regulatorios. Este enfoque optimiza el tiempo de auditoría y fortalece el juicio técnico.

El muestreo debe justificarse metodológicamente.

Sabías que:
Auditar controles de bajo riesgo sin revisar los críticos puede distorsionar conclusiones.

Autoevaluación:
¿Tu estrategia de muestreo prioriza impacto potencial?

◇ 3.6 Evaluación de Eficacia (C11)

Diseño vs Implementación vs Resultado

Evaluar eficacia requiere analizar tres niveles:

1. Diseño adecuado del control.
2. Implementación consistente en operación.
3. Resultado observable en reducción de riesgo.

Un control puede estar bien diseñado pero mal ejecutado, o ejecutado pero ineficaz.

Sabías que:
El examen evalúa esta distinción con casos situacionales (Dom. C).

Autoevaluación:
¿Puedes clasificar una falla como de diseño o de operación?

Evidencia Suficiente y Apropiada

La evaluación de eficacia exige evidencia verificable: registros, métricas, actas, validaciones independientes. La evidencia debe ser suficiente (cantidad adecuada) y apropiada (calidad relevante y confiable).

Sin evidencia objetiva, no existe conclusión defendible.

Sabías que:
Evidencia anecdótica o verbal no cumple estándar ISO 19011.

Autoevaluación:
¿La evidencia analizada permite concluir reducción real del riesgo?

Caso: Control Declarado pero No Operativo

Una organización declara en la SoA el control “supervisión humana obligatoria en decisiones críticas”.
En auditoría se observa:

- Procedimiento documentado.
- No existen registros de revisión humana.
- Actualización reciente del modelo sin gestión formal de cambio.
- Riesgo residual declarado como “aceptable”.

Autoevaluación:
¿El problema es de diseño, implementación o eficacia?

Resolución Técnica del Caso

Análisis auditor:

- Diseño: Adecuado (documentado).
- Implementación: Deficiente (sin registros).
- Resultado: Ineficaz (no se demuestra mitigación).

Cláusulas impactadas:

- 8.1 Control operacional
- 6.1.3 Tratamiento del riesgo
- Competencia C11 (evaluación de eficacia)

Clasificación probable: No Conformidad Mayor por falla sistémica de operación.

Autoevaluación:
¿Podrías defender esta clasificación ante comité de dirección?

Plantilla Recomendada – Evaluación Integral de Control

Control	Riesgo Asociado	Diseño	Evidencia Operación	Métrica Resultado	Conclusión
Supervisión humana	Sesgo crítico	Sí	No registros	No medido	Ineficaz
Gestión de cambios	Riesgo técnico	Parcial	Sin acta aprobación	No validado	Deficiente

Nota: Herramienta recomendada para práctica formativa. No es formato obligatorio normativo.

Autoevaluación Final:
¿Tu análisis diferencia claramente entre debilidad documental y falla operativa real?

Cierre del Módulo 3: De la Aplicabilidad a la Eficacia

En este módulo comprendiste que el verdadero valor del auditor interno del SGIA radica en evaluar si los controles seleccionados son pertinentes, están implementados y realmente reducen riesgos. La diferencia entre “cumplimiento documental” y “eficacia real” define la madurez del sistema.

En el siguiente módulo profundizaremos en medición, análisis y evaluación del desempeño del SGIA.

Autoevaluación Final del Módulo:
¿Tu criterio auditor se basa en evidencia objetiva o en confianza organizacional?

MÓDULO 4 — Evaluación del Desempeño (Cláusula 9 ISO/IEC 42001)

Enfoque: Dom. B (C5, C6, C7)

Transición: de controles eficaces a sistema eficaz

En el Módulo 3 validaste controles individuales (aplicabilidad y eficacia). Ahora el auditor debe juzgar el **desempeño global del SGIA**: qué se mide, con qué método, con qué frecuencia y qué decisiones se toman. La Cláusula 9 exige convertir datos y evidencias en conclusiones defendibles sobre eficacia y mejora continua.

Sabías que: Un SGIA puede "cumplir" controles y aun así fallar por falta de seguimiento y análisis.
Autoevaluación: ¿Qué fuentes integrarías antes de afirmar "el SGIA es eficaz"?

◇ 4.1 Qué evaluar (2)

SGIA vs sistema IA: dos niveles, dos juicios

El auditor debe separar el desempeño **técnico** del sistema IA (precisión, deriva, sesgo) del desempeño **del SGIA** (gobernanza, riesgos, cumplimiento, mejora). Un

modelo “bueno” puede estar mal gestionado. En auditoría, el criterio principal es el sistema de gestión y su capacidad de control y aprendizaje.

Sabías que: Confundir niveles conduce a hallazgos irrelevantes o conclusiones sin criterio.

Autoevaluación: ¿Qué evidencia te muestra “gestión” y no solo “rendimiento del modelo”?

Indicadores del SGIA: evidencia de control y aprendizaje

Los indicadores del SGIA deben demostrar logro de objetivos, gestión de riesgos y capacidad de mejora. El auditor verifica que existan KPI/KRI con responsables, umbrales y acciones asociadas. Si los indicadores solo describen actividad (“nº de reportes”) y no control (“reducción de riesgo”), el juicio de eficacia queda debilitado.

Sabías que: Indicadores sin umbral no activan decisiones; solo “informan”.

Autoevaluación: ¿Tus indicadores permiten decidir, o solo reportar?

4.2 9.1 Seguimiento y medición (6)

9.1 Qué medir: relevancia basada en riesgos

La organización debe determinar **qué** monitorear y medir para asegurar eficacia del SGIA. El auditor evalúa si lo medido se vincula con riesgos críticos, impactos y objetivos. Medir “lo fácil” en vez de “lo importante” crea ceguera operacional. La selección de métricas debe justificarse por criticidad y contexto.

Sabías que: El “set” de métricas es parte del diseño del control del sistema, no un accesorio.

Autoevaluación: ¿Qué riesgo crítico quedaría invisible si no se mide?

9.1 Métodos: definiciones, fórmulas y supuestos

No basta con tener un número; debe existir un método definido: fórmula, población, periodo, fuente, limpieza de datos y supuestos. El auditor revisa si el método es consistente y reproducible. Si el método cambia sin control, las tendencias dejan de ser comparables y el SGIA pierde capacidad de aprendizaje.

Sabías que: "Misma métrica, distinto método" = evidencia no confiable.
Autoevaluación: ¿Qué pedirías para probar que el método es reproducible?
Footer: Licensed under CC BY 4.0.

9.1 Frecuencia: intervalos planificados según riesgo

La organización debe definir **cuándo** medir, con qué frecuencia y bajo qué disparadores (cambios, incidentes, deriva). El auditor contrasta frecuencia planificada con criticidad del sistema IA y riesgos asociados. Si se mide tarde, el riesgo residual puede crecer silenciosamente y la organización pierde capacidad de respuesta oportuna.

Sabías que: Alta criticidad suele exigir mayor cadencia o monitoreo continuo.
Autoevaluación: ¿La frecuencia se ajusta al nivel de impacto del sistema?
Footer: Licensed under CC BY 4.0.

9.1 Registros: trazabilidad y control documental

Toda medición debe generar registros: fecha, responsable, fuente, resultado, evidencia de revisión y acciones. El auditor valida integridad, retención y control de versiones. Sin registro, no hay evidencia; sin control documental, la evidencia es discutible. Los registros deben permitir reconstruir decisiones y justificar cambios en riesgo o controles.

Sabías que: Registro incompleto = evidencia insuficiente, aun si "se midió".
Autoevaluación: ¿El registro permite auditar el "por qué" de una decisión?

9.1 Análisis: de métricas a conclusiones

Medir no equivale a evaluar. La organización debe analizar resultados para identificar tendencias, desviaciones y causas probables. El auditor revisa si existen criterios de interpretación, umbrales de alerta y seguimiento de anomalías. Sin análisis, el SGIA se vuelve reactivo: detecta tarde y corrige sin aprendizaje estructurado.

Sabías que: Un tablero sin análisis es "reporting", no "gestión".
Autoevaluación: ¿Qué evidencia demuestra que se analizan tendencias y no solo valores?

9.1 Acción: retroalimentación hacia riesgos y controles

La evaluación del desempeño debe activar acciones: ajustar controles, actualizar riesgos, revisar SoA, reentrenar, detener despliegues o reforzar supervisión humana. El auditor busca trazabilidad "dato → decisión → acción → verificación". Si no hay acciones, el SGIA no mejora: solo observa. La eficacia se demuestra con decisiones oportunas.

Sabías que: "Ninguna acción" ante desviaciones recurrentes suele indicar falla sistémica.
Autoevaluación: ¿Puedes rastrear una acción correctiva desde un indicador crítico?

4.3 Métricas específicas de IA (8)

Precisión: valor, límites y umbrales operativos

La precisión (u otras métricas predictivas) es útil si se monitorea en operación y tiene umbrales definidos. El auditor evalúa si la organización mide rendimiento en datos reales, detecta degradación y activa revisión de riesgos o cambios controlados. Precisión alta en pruebas no garantiza desempeño estable: sin monitoreo, el riesgo se oculta.

Sabías que: Métrica sin umbral = sin criterio para decidir.
Autoevaluación: ¿Qué evidencia mostraría que la precisión "gatilla" acciones?

Sesgo: medición, grupos y trazabilidad de mitigaciones

El sesgo requiere definir grupos, método de comparación y criterios de aceptación. El auditor valida si se mide equidad con periodicidad, si existe evaluación de impacto cuando aplica y si las mitigaciones quedan registradas. Declarar "equidad" sin medición es incoherencia con política/objetivos. El sesgo debe conectarse con riesgos y controles.

Sabías que: Sesgo no medido suele ser "riesgo no gestionado", no solo "dato faltante".
Autoevaluación: ¿La organización define grupos y umbrales de equidad?

Robustez: pruebas ante perturbaciones y escenarios adversos

La robustez evalúa estabilidad del sistema ante ruido, cambios de entrada o condiciones extremas. El auditor busca evidencia de pruebas periódicas, criterios de aprobación y acciones ante fallos. Robustez también incluye resiliencia operacional:

degradación controlada, límites de uso y mecanismos de contención. Sin pruebas, el control es presuntivo.

Sabías que: Robustez sin registros es “confianza”, no evidencia.
Autoevaluación: ¿Qué prueba demostraría robustez en un escenario de datos anómalos?

Deriva: detección temprana y control del ciclo de vida

La deriva ocurre cuando cambian datos, contexto o comportamiento del modelo. El auditor verifica monitoreo de deriva, umbrales, alertas y decisiones: recalibrar, reentrenar, restringir uso o retirar. Si hay deriva y no hay respuesta documentada, la evaluación de riesgos queda desactualizada y el SGIA pierde control operacional.

Sabías que: Deriva persistente sin acción suele ser evidencia de ineficacia del control.
Autoevaluación: ¿Cómo demostrarías que la deriva activa revisión de riesgo y SoA?

Explicabilidad: capacidad de justificar decisiones relevantes

La explicabilidad no exige revelar “todo el modelo”, sino poder justificar resultados cuando el contexto lo requiere (clientes, reguladores, usuarios). El auditor revisa mecanismos definidos, registros de explicaciones entregadas y controles de consistencia. Explicar también es un control: reduce riesgo reputacional y apoya cumplimiento. Sin proceso, hay improvisación.

Sabías que: Explicabilidad sin procedimiento es vulnerable ante incidentes o reclamos.
Autoevaluación: ¿Qué evidencia pedirías para demostrar “explicación

consistente"?
Footer: Licensed under CC BY 4.0.

Calidad de datos: base de métricas y riesgo

Muchas métricas dependen de datos confiables. El auditor evalúa si existen controles de calidad, procedencia y representatividad de datos usados para medir (no solo para entrenar). Si los datos de monitoreo están sesgados o incompletos, las conclusiones de desempeño son inválidas. La organización debe demostrar que mide sobre datos pertinentes al contexto real.

Sabías que: "Mala data" puede simular estabilidad o esconder degradación.
Autoevaluación: ¿Cómo verificarías la representatividad del set de monitoreo?
Footer: Licensed under CC BY 4.0.

KPI/KRI de IA: vincular técnica con gobernanza

Las métricas técnicas deben traducirse a riesgos y decisiones: umbrales, responsables, acciones y verificación posterior. El auditor revisa si un KPI/KRI de IA alimenta objetivos del SGIA y tratamiento del riesgo. Si el tablero técnico no se conecta con la gestión, el SGIA se vuelve "observador", no "controlador".

Sabías que: Una métrica técnica sin dueño es un riesgo de gobernanza.
Autoevaluación: ¿Quién decide acciones cuando un KPI técnico se degrada?
Footer: Licensed under CC BY 4.0.

Métricas de proceso: incidentes, cambios, excepciones

Además de métricas del modelo, el auditor evalúa métricas del proceso: incidentes de IA, cambios no planificados, excepciones a supervisión humana, retrabajos y tiempos de respuesta. Estas métricas evidencian la "salud operativa" del SGIA. Si el

sistema tiene incidentes repetidos y no aprende, la eficacia global es cuestionable, aunque el modelo rinda bien.

Sabías que: Reincidencia de incidentes suele apuntar a fallas de mejora (y gestión).
Autoevaluación: ¿Qué métrica de proceso te ayudaría a detectar control ineficaz?
Footer: Licensed under CC BY 4.0.

◇ 4.4 Validez/fiabilidad (C5) (6)

C5 Validez: ¿la métrica mide lo que dice medir?

Validez implica que el indicador refleja el fenómeno relevante. El auditor revisa definiciones, población, sesgos del set de evaluación y coherencia con objetivos. Una métrica puede ser precisa estadísticamente pero inválida para el riesgo (p.ej., mide "precisión global" e ignora subgrupos). Sin validez, cualquier conclusión de desempeño es frágil.

Sabías que: Validez deficiente produce "decisiones correctas con datos incorrectos".
Autoevaluación: ¿Qué evidencia usarías para cuestionar la validez de una métrica?
Footer: Licensed under CC BY 4.0.

C5 Fiabilidad: consistencia y estabilidad del método

Fiabilidad es consistencia del resultado bajo el mismo método. El auditor valida control de versiones del código/método, estabilidad de fuentes de datos y repetibilidad. Si el indicador cambia por ajustes no controlados, la tendencia no es confiable. Una organización madura demuestra reproducibilidad y control de cambios en sus métricas, igual que en sus modelos.

Sabías que: "Métrica que cambia sin trazabilidad" es una señal de control débil.
Autoevaluación: ¿Cómo verificarías repetibilidad sin re-ejecutar todo el pipeline?
Footer: Licensed under CC BY 4.0.

C5 Trazabilidad: fuente, transformación y custodia del dato

El auditor debe poder seguir la ruta “dato origen → transformación → cálculo → reporte”. Revisa linaje, logs, repositorios y custodios. Sin trazabilidad, el número es una caja negra y no se puede defender en auditoría. La trazabilidad también soporta responsabilidad: quién produjo, quién aprobó y quién interpretó el resultado.

Sabías que: La trazabilidad reduce disputas: convierte debate en verificación.

Autoevaluación: ¿Qué artefacto probaría linaje del dato de monitoreo?

Footer: Licensed under CC BY 4.0.

C5 Dueños de métricas: accountability y segregación

Cada indicador debe tener dueño responsable, con roles claros para definir, calcular, revisar y aprobar. El auditor evalúa segregación razonable para evitar “auto-validación” del mismo equipo. Sin dueños, las métricas se vuelven huérfanas: nadie responde por su calidad o por decisiones tardías. La responsabilidad formal es evidencia de control de gestión.

Sabías que: Métrica sin dueño suele correlacionar con falta de acción ante alertas.

Autoevaluación: ¿Quién aprueba cambios de método en métricas críticas?

Footer: Licensed under CC BY 4.0.

C5 Sesgos de medición: cuando el indicador engaña

El auditor debe considerar sesgos en muestreo, selección de datos, métricas agregadas y “promedios” que ocultan subgrupos. Revisa si la organización evalúa desempeño por segmentos relevantes y si documenta limitaciones del indicador. Si el sesgo de medición no se reconoce, el SGIA puede declarar eficacia mientras aumenta el riesgo real.

Sabías qué: Promedios altos pueden esconder fallos graves en poblaciones minoritarias.
Autoevaluación: ¿Qué segmentación pedirías para evitar "falsa seguridad"?

C5 Cierre: aceptar conclusiones solo si el método es sólido

Antes de aceptar "cumplimos el objetivo", el auditor valida método, datos, trazabilidad y responsables. Si el método es débil, la conclusión es inválida aunque el número parezca bueno. El juicio auditor se basa en evidencia defendible, no en resultados aislados. La eficacia del SGIA requiere confianza justificada en la medición, no confianza ciega.

Sabías que: En auditoría, método débil = evidencia insuficiente.
Autoevaluación: ¿Qué criterio usarías para rechazar una métrica como evidencia?

4.5 Intervalos planificados (C6) (5)

C6 Intervalos: lo planificado debe ejecutarse y evidenciarse

C6 evalúa si las mediciones y revisiones ocurren en intervalos planificados. El auditor revisa calendarios, reportes, logs y firmas de revisión. Si la cadencia se incumple, el sistema pierde capacidad de detección temprana. La periodicidad debe ser coherente con criticidad: medir tarde equivale a tratar riesgos tarde, aumentando exposición operativa y regulatoria.

Sabías que: "Se iba a medir" no es evidencia; el registro de ejecución sí.
Autoevaluación: ¿Qué documento prueba periodicidad sin discusión?

C6 Brechas: evaluar magnitud, recurrencia e impacto

No toda brecha tiene el mismo peso. El auditor analiza duración del atraso, recurrencia y riesgo asociado. Un atraso en métrica crítica (sesgo/deriva) puede ser grave; un atraso aislado en métrica menor podría ser OM. La conclusión debe justificar el impacto: qué decisión se retrasó y qué riesgo aumentó. Sin análisis de impacto, el hallazgo es débil.

Sabías que: La gravedad crece cuando la brecha afecta decisiones de control.
Autoevaluación: ¿Cómo decidirías entre NC y OM ante un atraso?
Footer: Licensed under CC BY 4.0.

C6 Evidencia: del cronograma al cumplimiento real

El auditor compara “planificado” vs “ejecutado”: fechas, responsables, evidencia de revisión y entrega de informes. También valida si existen mecanismos para reprogramar con aprobación y justificar excepciones. Si se reprograma sin control, el intervalo pierde significado. La evidencia debe permitir reconstruir el historial de cumplimiento, no solo el estado actual.

Sabías que: Reprogramaciones repetidas pueden ser señal de falta de recursos o gobernanza.
Autoevaluación: ¿Qué evidencia pedirías cuando alegan “falta de tiempo”?
Footer: Licensed under CC BY 4.0.

C6 Coherencia: la cadencia debe seguir el riesgo y el cambio

La frecuencia debe ajustarse ante cambios significativos: nuevas versiones del modelo, nuevos datos, incidentes, cambios regulatorios. El auditor verifica si la organización “aumenta el monitoreo” cuando el riesgo crece. Si la cadencia

permanece igual pese a cambios, hay debilidad de control adaptativo. Un SGIA eficaz aprende y ajusta su vigilancia según contexto.

Sabías que: Cambios sin ajuste de cadencia suelen anticipar incidentes.
Autoevaluación: ¿Qué cambio exigiría incrementar monitoreo inmediatamente?
Footer: Licensed under CC BY 4.0.

▧ C6 Cierre: intervalo incumplido como señal de ineficacia

Cuando los intervalos no se cumplen, el auditor evalúa si es un síntoma aislado o sistémico: recursos insuficientes, prioridades erróneas o falta de liderazgo. La conclusión debe conectar brecha con riesgo: qué quedó sin observar y qué decisión se dejó de tomar. El foco no es castigar el atraso, sino demostrar cómo afecta la eficacia del SGIA y la exposición al riesgo.

Sabías que: Intervalos incumplidos recurrentes suelen escalar a NC por sistema, no por evento.
Autoevaluación: ¿Cómo demostrarías "impacto en riesgo" con evidencia?
Footer: Licensed under CC BY 4.0.

◇ 4.6 Integración para juicio de eficacia (C7) (5)

▧ C7 Integración: una historia única con varias fuentes

C7 exige integrar evidencias: métricas, auditorías internas, no conformidades, incidentes y revisión por dirección. El auditor busca coherencia: ¿las métricas confirman lo que dicen las auditorías? ¿las NC se repiten? ¿las decisiones de dirección se basan en datos? Si las fuentes se contradicen, el sistema puede estar "reportando" sin controlar. Integrar es convertir señales en juicio.

Sabías que: La inconsistencia entre fuentes es hallazgo de madurez del sistema.
Autoevaluación: ¿Qué harías si el tablero dice "todo bien" y hay incidentes

crecientes?
Footer: Licensed under CC BY 4.0.

C7 Tendencias: evidenciar mejora o deterioro sostenido

La eficacia global se aprecia en tendencias, no en "fotografías". El auditor analiza series temporales: recurrencia de incidentes, desviaciones persistentes, mejora posterior a acciones correctivas. Si no hay tendencia, no hay aprendizaje. Un SGIA eficaz muestra reducción de riesgo, estabilización de métricas y cierre oportuno de acciones. La tendencia es evidencia de control adaptativo y mejora continua.

Sabías que: Mejorar = reducir recurrencia, no solo "cerrar tickets".
Autoevaluación: ¿Qué tendencia te haría concluir ineficacia sistémica?
Footer: Licensed under CC BY 4.0.

C7 Coherencia con política y objetivos: cumplir lo prometido

El auditor contrasta resultados con los compromisos de la política y objetivos. Si la política declara "equidad" y no se mide sesgo, hay incoherencia estratégica. Si los objetivos exigen mejorar la robustez y no hay pruebas, la eficacia global se cuestiona. C7 exige evaluar alineación: no basta con medir; debe medirse lo que importa para la promesa organizacional y su perfil de riesgo.

Sabías que: La coherencia es "control de gestión": conecta intención con evidencia.
Autoevaluación: ¿Qué evidencia muestra alineación entre objetivos y métricas realmente usadas?
Footer: Licensed under CC BY 4.0.

C7 Juicio global: criterios para concluir eficacia del SGIA

El auditor debe emitir una conclusión defendible: eficaz, parcialmente eficaz o ineficaz. Para ello integra calidad de métodos (C5), cumplimiento de intervalos (C6) y coherencia multifuente (C7). La conclusión debe estar trazada a evidencias específicas, no a impresiones. Un buen juicio explica "por qué" y "qué implica": nivel de confianza, riesgos residuales y prioridades de mejora.

Sabías que: Una conclusión sin trazabilidad es vulnerable ante discusión con dirección.
Autoevaluación: ¿Puedes sostener tu conclusión citando evidencias y no opiniones?

Puente hacia 9.2 y 9.3: evaluación del desempeño como sistema

La evaluación del desempeño no termina en métricas: se completa con auditoría interna (9.2) y revisión por la dirección (9.3). El auditor analiza si las métricas alimentan auditorías (enfoque basado en riesgo) y si la dirección toma decisiones informadas. Si la auditoría y la dirección no usan resultados, el sistema pierde el "Check" del PDCA y queda sin aprendizaje organizacional.

Sabías que: Medición sin revisión directiva es "dato sin gobierno".
Autoevaluación: ¿Cómo probarías que dirección usa métricas para decidir?

◇ 4.7 9.3 Revisión por la dirección (4)

9.3 Propósito: asegurar idoneidad, adecuación y eficacia

La revisión por la dirección evalúa si el SGIA sigue siendo adecuado al contexto, idóneo para objetivos y eficaz para controlar riesgos. El auditor busca evidencia de revisión periódica: agenda, entradas, análisis y decisiones. Si la dirección "se reúne" pero no revisa datos críticos, la revisión es formalista y no cumple su función de gobierno. La revisión es un control de alto nivel.

Sabías que: Revisión sin decisiones documentadas suele ser evidencia débil.
Autoevaluación: ¿Qué evidencia demuestra que la revisión fue real y no ceremonial?

9.3 Entradas: qué debe revisar la dirección con evidencia

El auditor verifica las entradas típicas: resultados de medición, auditorías, NC/AC, incidentes, cambios en contexto/regulación, desempeño de proveedores y estado de riesgos. La pregunta clave: ¿se revisó lo crítico para el negocio y para las partes interesadas? Si faltan entradas relevantes (sesgo, deriva, impactos), la dirección no gobierna el riesgo real.

Sabías que: Entradas incompletas sesgan decisiones y pueden aumentar riesgo residual.
Autoevaluación: ¿Qué entrada considerarías "no negociable" para IA de alto impacto?

9.3 Salidas: decisiones, recursos y seguimiento verificable

La revisión debe producir salidas: decisiones, acciones, cambios en política/objetivos, reasignación de recursos y prioridades. El auditor verifica trazabilidad: salida → responsable → fecha → verificación de eficacia. Sin seguimiento, la revisión pierde valor y el SGIA no mejora. Las salidas deben responder a tendencias y brechas; si se repiten problemas, la dirección debe evidenciar escalamiento.

Sabías que: Sin seguimiento, la revisión se convierte en “acta” sin control.
Autoevaluación: ¿Cómo demostrarías que una decisión se implementó y fue eficaz?

◇ CASO INTEGRADOR + RESOLUCIÓN + PLANTILLA (C5–C7)

▧ Caso integrador: métricas “buenas” y gobierno débil

La organización reporta precisión alta y estable, pero no mide sesgo ni deriva por subgrupos, y la frecuencia real de medición se incumple en métricas críticas. Auditorías internas se retrasan y la revisión por la dirección solo recibe un tablero resumido sin análisis de brechas. El auditor debe decidir si el SGIA es eficaz o si existe falla sistémica por C5 (método), C6 (intervalos) y C7 (integración).

Sabías que: Buen rendimiento técnico puede ocultar riesgo no gobernado.
Autoevaluación: ¿Qué evidencia pedirías primero: método, cronograma o acta de revisión?

▧ Resolución modelo auditor: diagnóstico y conclusión defendible

Diagnóstico: hay evidencia parcial de desempeño técnico, pero falla la evaluación del desempeño del SGIA. C5: validez incompleta (no segmenta sesgo). C6: intervalos incumplidos en métricas críticas. C7: integración débil (dirección no analiza ni decide con base en evidencias completas). Conclusión: SGIA **parcialmente eficaz** con debilidades sistémicas; requiere correcciones en medición, cadencia y gobernanza.

Sabías que: "Parcialmente eficaz" exige justificar riesgos residuales y plan de mejora.
Autoevaluación: ¿Qué haría que cambies la conclusión a "ineficaz"?

Plantilla recomendada: matriz de juicio integrado (C5–C7)

Usa esta matriz formativa para integrar evidencia y sostener tu conclusión. Evalúa calidad del método, cumplimiento de intervalos y coherencia multifuente antes de concluir eficacia global. La clave es transformar evidencias dispersas en una narrativa verificable: qué está bien, qué falta, qué riesgo aumenta y qué decisión se requiere. Esta plantilla no es obligatoria por la norma; es recomendación de práctica auditor.

Sabías que: Una matriz reduce sesgo del auditor y mejora consistencia entre auditores.
Autoevaluación: ¿Qué columna agregarías para reforzar trazabilidad a cláusulas específicas?

Matriz (recomendada):

Dimensión	Evidencia	Calidad	Intervalo	Riesgo/Impacto	Decisión/Acción
C5 Método	Definición + fórmula + dataset	Alta/Media/Baja	N/A	Alto/Medio/Bajo	Ajustar método
C6 Cadencia	Calendario + logs + reportes	Alta/Media/Baja	Cumple/No	Alto/Medio/Bajo	Reprogramar y controlar

C7 Integración	Auditoría + NC + dirección	Alta/Media/Baja	N/A	Alto/Medio/Bajo	Escalar y decidir

Cierre del Módulo 4: listo para auditar el “Check” del SGIA

En este módulo aprendiste a evaluar desempeño del SGIA con rigor: seleccionar qué medir, validar métodos (C5), confirmar intervalos planificados (C6) e integrar fuentes para concluir eficacia global (C7). El siguiente paso es auditar formalmente el proceso 9.2 con ISO 19011: programa, plan, muestreo, evidencia y hallazgos. Aquí pasas de “analizar desempeño” a “auditar el sistema” con metodología.

Sabías que: Un buen auditor explica el “por qué” con evidencia, no con opiniones.
Autoevaluación: ¿Puedes defender tu conclusión ante dirección citando evidencias concretas?

MÓDULO 5

Auditoría Interna del SGIA (ISO 19011 + 9.2 ISO/IEC 42001)

Enfoque: Dom. A (C1, C2, C3, C4)
Objetivo: ejecutar auditorías internas del SGIA con imparcialidad, criterios claros, muestreo basado en riesgo y evidencia objetiva suficiente y apropiada

Transición: Evaluar vs Auditar (9.1 vs 9.2)

Contenido principal (≤300):
Evaluar desempeño (9.1) describe resultados; auditar (9.2) determina conformidad y eficacia del SGIA frente a criterios. Como auditor, cambias de "leer indicadores" a "probar control": plan, método, muestreo, evidencia verificable y conclusión defendible.

Sabías que:
ISO 19011 muestra el flujo típico: recopilar información, verificarla, convertirla en evidencia y evaluarla contra criterios para producir hallazgos y conclusiones. Esta lógica evita conclusiones basadas en intuición.

Autoevaluación:
Si una métrica "sale bien", ¿qué evidencia adicional necesitas para concluir conformidad con 9.2 y no solo buen desempeño?

Principio: Integridad

Contenido principal (≤300):
La integridad es la base del profesionalismo del auditor: actuar éticamente, con honestidad y responsabilidad, resistiendo influencias sobre el juicio. En SGIA, esto implica registrar hechos relevantes aunque sean incómodos y sostener trazabilidad entre evidencia y hallazgo.

Sabías que:
ISO 19011 establece que la adhesión a los principios es requisito previo para conclusiones pertinentes y suficientes. Sin integridad, la evidencia puede existir, pero la auditoría pierde credibilidad.

Autoevaluación:
¿Qué harías si el auditado ofrece "arreglarlo después" a cambio de no registrar un hallazgo hoy?

Principio: Presentación imparcial

Contenido principal (≤300):
Presentación imparcial exige informar con veracidad y exactitud: hallazgos, conclusiones e informe deben reflejar lo auditado. El auditor separa criterio, condición y evidencia; y registra obstáculos y desacuerdos. La claridad protege la validez del informe ante revisión.

Sabías que:
ISO 19011 exige que la comunicación sea veraz, exacta, objetiva, oportuna, clara y completa. En auditoría IA, esto reduce discusiones "opinión vs opinión" y las convierte en verificación.

Autoevaluación:
¿Cómo redactarías un hallazgo para que otro auditor llegue a la misma conclusión con la misma evidencia?

Principio: Debido cuidado profesional

Contenido principal (≤300):
Debido cuidado es aplicar diligencia y juicio razonado según la importancia del proceso auditado. En IA, evita conclusiones rápidas por complejidad técnica: define qué es suficiente, cuándo escalar dudas y cómo manejar incertidumbre sin perder objetividad.

Sabías que:
ISO 19011 señala que un factor clave del debido cuidado es la capacidad de emitir juicios razonados en situaciones de auditoría. Esto se traduce en "no concluir sin evidencia suficiente y apropiada".

Autoevaluación:
¿Con qué criterio decides ampliar muestra o solicitar evidencia adicional antes de cerrar una conclusión?

Principio: Confidencialidad

Contenido principal (≤300):
Confidencialidad es seguridad de la información: usar y proteger datos, modelos, evidencias y hallazgos con discreción. En SGIA, muchas evidencias contienen información sensible; la custodia correcta sostiene confianza y evita daño a intereses legítimos del auditado.

Sabías que:
ISO 19011 indica que la información de auditoría no debe usarse inapropiadamente ni de forma perjudicial, incluyendo el tratamiento de información sensible/confidencial.

Autoevaluación:
¿Qué controles aplicarías para almacenar evidencias (datasets, logs, capturas) sin exponer datos personales?

Principio: Independencia

Contenido principal (≤300):
Independencia es base de imparcialidad y objetividad. El auditor debe estar libre de sesgo y conflicto; en auditorías internas, ser independiente de la función auditada en lo posible. En SGIA, evita auditar controles que diseñaste o aprobaste sin mitigación formal.

Sabías que:
ISO 19011 indica que los hallazgos y conclusiones deben basarse solo en evidencia y que, si no hay independencia plena, deben hacerse esfuerzos para eliminar sesgo.

Autoevaluación:
Si participaste en el diseño de un control del SGIA, ¿qué mitigación documentada aplicarías para auditarlo?

C1: Programa de auditoría (visión y priorización)

Contenido principal (≤300):
El programa define auditorías planificadas, frecuencia y recursos. En SGIA debe priorizar por riesgo, cambios (modelo/datos/proveedor) y resultados previos. Como auditor, validas que el programa no sea "calendario", sino mecanismo vivo de control del riesgo organizacional.

Sabías que:
Un programa eficaz alinea el esfuerzo auditor con incertidumbre y exposición real. Si el riesgo cambia, el programa debe adaptarse; si no, la auditoría se vuelve "cumplimiento de agenda" sin valor.

Autoevaluación:
¿Qué 3 disparadores (riesgo/cambio/incidente) justificarían replanificar el programa anual del SGIA?

C1: Priorización por riesgo, cambios y resultados previos

Contenido principal (≤300):
Priorizas donde el SGIA puede fallar: sistemas IA de alto impacto, controles críticos, cambios recientes y reincidencia de hallazgos. El auditor justifica frecuencia y alcance con evidencia (incidentes, desviaciones, auditorías previas), evitando "auditar lo fácil" y omitir lo crítico.

Sabías que:
La recurrencia indica que el sistema no aprende. Priorizar por reincidencia mejora la eficacia del programa y acelera la reducción del riesgo residual.

Autoevaluación:
Ante dos procesos: uno "ordenado" pero crítico y otro "desordenado" pero menor, ¿cuál priorizas y con qué evidencia lo justificas?

C1: Recursos y competencia del equipo auditor

Contenido principal (≤300):
El programa debe asignar auditores competentes y tiempo suficiente. En SGIA, la competencia incluye comprender ciclo de vida IA, riesgos, controles y evidencia técnica mínima (logs, métricas, cambios). Sin competencia, el auditor acepta narrativas sin verificación y debilita conclusiones.

Sabías que:
La competencia soporta el principio de debido cuidado. Si el equipo no domina lo esencial, aumenta el riesgo de "falsos conformes" y de no detectar fallas sistémicas.

Autoevaluación:
¿Qué perfiles o conocimientos mínimos exigirías para auditar un sistema IA de alto impacto (sin pedir "ser data scientist")?

C1: Seguimiento del programa y control de ejecución

Contenido principal (≤300):
El programa se controla comparando planificado vs ejecutado: auditorías realizadas, reprogramaciones, causas y acciones. El auditor verifica trazabilidad de decisiones (por qué se movió una auditoría crítica) y evidencia de revisión periódica. Reprogramación repetida puede ser señal de gobernanza débil.

Sabías que:
Si las auditorías no ocurren como se planifican, el SGIA pierde su mecanismo interno de detección. El seguimiento del programa es, en sí, un control de gestión.

Autoevaluación:
¿Qué evidencia pedirías para concluir que el programa de auditoría es eficaz (no solo "existe")?

C2: Plan de auditoría (de intención a ejecución)

Contenido principal (≤300):
El plan convierte el programa en una auditoría ejecutable: define objetivos, criterios, alcance, métodos, muestreo, roles y agenda. Como auditor, aseguras que el plan habilite evidencia suficiente y apropiada y reduzca ambigüedad: lo no planificado se audita por excepción, no por improvisación.

Sabías que:
ISO 19011 exige que la evidencia se evalúe contra criterios para determinar hallazgos; por eso, "criterios claros" y "alcance definido" son el corazón del plan.

Autoevaluación:
Si el plan no define criterios explícitos, ¿qué riesgo introduces en la validez de tus hallazgos?

C2: Alcance, límites y exclusiones justificadas

Contenido principal (≤300):
El alcance delimita procesos, periodo, ubicaciones y sistemas IA incluidos. Exclusiones deben justificarse por contexto/riesgo, no por conveniencia. El auditor valida que el alcance cubra interfaces críticas (datos, proveedores, operación) para evitar conclusiones "parciales" presentadas como globales.

Sabías que:
Un alcance estrecho puede producir un informe "positivo" sin proteger a la organización. La buena práctica es probar que lo excluido no cambia materialmente el juicio de eficacia.

Autoevaluación:
¿Qué pregunta usarías para detectar una exclusión "cómoda" que oculta un riesgo alto?

C2: Métodos y muestreo (enfoque basado en evidencia)

Contenido principal (≤300):
El plan define métodos (documentos, entrevistas, observación) y muestreo basado en riesgo. El auditor decide tamaño y foco de muestra para maximizar evidencia en tiempo finito. La evidencia debe ser verificable y normalmente se apoya en muestras; por eso, el muestreo debe justificarse.

Sabías que:
ISO 19011 establece que la evidencia debe ser verificable y, en general, se basa en muestras porque la auditoría tiene tiempo y recursos finitos. Además, la información recopilada debe verificarse en la medida de lo posible.

Autoevaluación:
¿Qué criterio usarías para seleccionar muestras cuando el riesgo está concentrado en cambios recientes del modelo?

C2: Plan de entrevistas (quién, por qué, qué validar)

Contenido principal (≤300):
El plan de entrevistas define roles clave (dueños de riesgo, operación, TI/ML, legal, proveedores) y el propósito de cada entrevista. El auditor prepara preguntas ligadas a criterios y evidencia esperada, evitando conversaciones generales que no demuestran conformidad ni eficacia.

Sabías que:
En ISO 19011, las entrevistas son un medio para obtener información, pero su valor aumenta cuando se verifica con registros y observación; así se reduce el sesgo de "lo que dicen" vs "lo que ocurre".

Autoevaluación:
¿Qué 3 preguntas harías para pasar de “explicación verbal” a “evidencia verificable” en una entrevista SGIA?

C2: Agenda y logística (tiempo finito, foco máximo)

Contenido principal (≤300):
La agenda define secuencia, tiempos, puntos de control y logística (reunión de apertura, recorridos, revisión de evidencias, cierre). El auditor asegura disponibilidad de evidencias y personas, y reserva tiempo para análisis. Una agenda realista evita auditorías “apresuradas” que producen conclusiones débiles.

Sabías que:
Una auditoría efectiva gestiona el tiempo como un recurso de riesgo: si faltan espacios para verificar, la evidencia se vuelve insuficiente y aumenta la probabilidad de “falsos conformes”.

Autoevaluación:
Si el auditado cambia la agenda el mismo día, ¿qué parte protegerías para no perder calidad de evidencia?

C2: Comunicación previa y preparación de evidencia

Contenido principal (≤300):
Antes de iniciar, el auditor comunica objetivos, criterios, alcance y evidencias requeridas (SoA, matriz de riesgos, métricas, cambios, actas). Esto reduce fricción y mejora eficiencia. La preparación no “entrena” al auditado; habilita que la auditoría mida realidad, no improvisación documental.

Sabías que:
ISO 19011 resalta la importancia de planificar considerando información disponible del programa y del auditado; una preparación clara mejora la verificabilidad de la evidencia y reduce interrupciones durante la ejecución.

Autoevaluación:
¿Qué documentos solicitarías antes para auditar eficacia de controles sin depender solo de entrevistas?

◇ 5.4 Imparcialidad y conflictos (C3) (4)

▨ C3: Identificar conflictos de interés (antes de auditar)

Contenido principal (≤300):
El auditor debe identificar conflictos: participación previa en diseño/operación, dependencia jerárquica, incentivos, relaciones con proveedores. La organización registra evaluación y decide mitigación (reasignación, supervisión, equipo mixto). Sin gestión de conflicto, la conclusión pierde legitimidad aunque la evidencia sea sólida.

Sabías que:
ISO 19011 destaca independencia como base de imparcialidad; cuando no es posible plena independencia, deben tomarse medidas para reducir sesgo y documentarlas.

Autoevaluación:
¿Qué conflicto sería "inaceptable" para ti en una auditoría del SGIA y por qué?

C3: Mitigar conflictos (controles de objetividad)

Contenido principal (≤300):
Mitigar no es "declarar" conflicto: es aplicar controles. Ejemplos: reasignar auditor, incorporar revisor independiente, rotar roles, restringir áreas, y registrar aprobación. El auditor debe asegurar que la mitigación sea proporcional al riesgo de sesgo, especialmente en hallazgos de alto impacto.

Sabías que:
La mitigación documentada protege al auditor y al auditado: reduce disputas sobre imparcialidad y fortalece confianza en el informe.

Autoevaluación:
Si no puedes reasignar al auditor, ¿qué control alterno aplicarías para sostener objetividad?

C3: Evidencia de independencia (no basta con afirmarla)

Contenido principal (≤300):
La independencia debe evidenciarse: declaraciones, matriz de conflictos, aprobación del líder del programa y registros de mitigación. El auditor verifica que el equipo no audite su propio trabajo. En SGIA, esto es crítico si el auditor participó en evaluación de riesgos, SoA o diseño de controles.

Sabías que:
Cuando el auditado cuestiona independencia, la respuesta no es "confía", sino mostrar evidencia documentada de evaluación y mitigación.

Autoevaluación:
¿Qué registro te gustaría ver en el expediente para defender independencia ante auditor externo?

▧ C3: Objetividad en el informe (lenguaje y trazabilidad)

Contenido principal (≤300):
La objetividad se refleja en cómo escribes: criterio citado, evidencia verificable, condición observada y conclusión. Evita adjetivos ("malo", "pobre") y usa hechos ("no existe registro", "no se cumplió intervalo"). Una redacción objetiva reduce conflictos y permite que el informe sea reproducible.

Sabías que:
ISO 19011 enfatiza presentación imparcial: comunicar con exactitud y basarse en evidencia; el lenguaje objetivo transforma desacuerdo en verificación.

Autoevaluación:
Reescribe un juicio subjetivo ("no gestionan bien cambios") en un hallazgo objetivo criterio–condición–evidencia.

◇ 5.5 Obtención y registro de evidencia (C4) (5)

▧ C4: Evidencia suficiente y apropiada (calidad y cantidad)

Contenido principal (≤300):
La evidencia debe ser suficiente (cantidad) y apropiada (calidad, relevancia y confiabilidad) para sostener hallazgos. El auditor evalúa verificabilidad y pertinencia al criterio. En IA, entrevistas sin registros rara vez bastan; se requieren logs, actas, métricas, aprobaciones y trazabilidad riesgo–control.

Sabías que:
ISO 19011 indica que la evidencia es verificable y generalmente se basa en muestras por recursos finitos; por eso el auditor debe justificar la suficiencia de su base de evidencia.

Autoevaluación:
¿Qué haría que clasifiques tu evidencia como "insuficiente" aunque el auditado responda bien?

C4: Triangulación (reducir sesgo y aumentar certeza)

Contenido principal (≤300):
Triangular es validar un hecho con al menos dos o tres fuentes: documento, entrevista y evidencia operacional (registro/observación). En SGIA, esto evita depender de narrativas y permite confirmar operación real del control. El auditor usa triangulación especialmente en controles críticos: cambios, supervisión humana, métricas, incidentes.

Sabías que:
ISO 19011 promueve verificar la información en la medida de lo posible; triangulación es la práctica que convierte información en evidencia robusta.

Autoevaluación:
Para un control de "monitoreo de sesgo", ¿qué 3 fuentes triangularías y por qué?

C4: Registro de evidencia (cadena de custodia auditora)

Contenido principal (≤300):
Registrar evidencia significa documentar fuente, fecha, responsable, ubicación, versión y vínculo al criterio. Esto permite trazabilidad y re-evaluación. En IA, el auditor debe registrar también contexto técnico mínimo (periodo de logs, versión del modelo, dataset de monitoreo) para evitar disputas posteriores sobre "qué se revisó".

Sabías que:
Un registro débil de evidencia convierte el informe en "relato"; un registro fuerte lo convierte en documento defendible.

Autoevaluación:
¿Qué dato técnico mínimo anotarías al capturar evidencia de un dashboard de métricas IA?

C4: Hallazgos (criterio–condición–evidencia–impacto)

Contenido principal (≤300):
Un hallazgo sólido declara el criterio (requisito), describe la condición (lo observado), cita evidencia verificable y explica impacto/riesgo. En SGIA, el impacto debe vincularse a riesgo residual, partes interesadas o incumplimiento de intervalos. Sin impacto, el hallazgo se percibe "menor" aunque sea crítico.

Sabías que:
ISO 19011 define hallazgos como resultado de evaluar evidencia frente a criterios; si el criterio no está claro, el hallazgo se vuelve opinable.

Autoevaluación:
¿Qué componente te falta cuando un hallazgo genera discusión: criterio, evidencia o impacto?

C4: Conclusiones e informe (de hallazgos a juicio global)

Contenido principal (≤300):
Las conclusiones integran hallazgos y evidencias para declarar conformidad, eficacia y oportunidades de mejora. El informe debe ser claro, trazable y consistente con la evidencia registrada. En IA, el auditor evita conclusiones absolutas sin base ("es seguro"), y reporta con alcance: "según evidencia revisada" y "en el periodo auditado".

Sabías que:
La claridad del informe protege la imparcialidad: otros deben poder seguir la lógica desde evidencia hasta conclusión sin "saltos".

Autoevaluación:
¿Cómo redactarías una conclusión eficaz sin exceder el alcance ni crear promesas implícitas?

◇ 5.6 Taller tipo examen: mini-casos (2)

▧ Mini-caso 1: SoA "actualizada" pero riesgo desalineado

Contenido principal (≤300):
La SoA muestra controles "implementados", pero la matriz de riesgos no refleja cambios recientes del modelo y no hay evidencia de revisión tras incidentes. Como auditor, debes decidir si el problema es trazabilidad, control operacional o evaluación del desempeño, y qué evidencia adicional recolectar antes de concluir.

Sabías que:
Cuando SoA y riesgos se contradicen, la auditoría debe buscar la "fuente de verdad" y reconstruir decisiones: qué cambió, quién aprobó y qué se actualizó.

Autoevaluación:
¿Qué 3 evidencias pedirías primero para validar trazabilidad riesgo → control → justificación?

▧ Mini-caso 2: Auditor sin independencia (auto-auditoría)

Contenido principal (≤300):
El auditor asignado diseñó el procedimiento de gestión de cambios que ahora audita. Se declara "independiente" por escrito, pero no existe mitigación adicional.

Debes decidir si la auditoría puede continuar, qué control compensatorio aplicar y cómo documentar la decisión para sostener imparcialidad ante revisión.

Sabías que:
La independencia es base de objetividad; si no se gestiona el conflicto, los hallazgos y conclusiones pueden ser cuestionados o invalidados.

Autoevaluación:
¿Qué mitigación mínima aplicarías para sostener objetividad y credibilidad del informe?

◇ MÓDULO 5 – ENTREGABLES DIDÁCTICOS (ARTEFACTOS)

Plantilla Programa de Auditoría (ISO 19011 / 9.2)

Contenido principal (≤300):
El programa de auditoría organiza auditorías planificadas según riesgo, cambios y resultados previos. Debe evidenciar priorización, recursos asignados y seguimiento. Esta plantilla facilita enfoque basado en riesgo y control de ejecución anual.

Plantilla editable:

Proceso / SGIA	Riesgo (Alto/Medio/Bajo)	Motivo de Prioridad	Fecha Plan	Auditor	Estado	Seguimiento

Sabías que:

ISO 19011 exige que el programa considere riesgos, cambios y resultados previos. Un programa no priorizado debilita el enfoque preventivo.

Autoevaluación:

¿Qué criterio adicional incluirías para reflejar criticidad del sistema IA?

Plantilla Plan de Auditoría (Objetivos/Criterios/Alcance/Muestreo)

Contenido principal (≤300):

El plan traduce el programa en auditoría ejecutable. Debe definir objetivos claros, criterios normativos, alcance preciso y método de muestreo basado en riesgo. Esta plantilla asegura trazabilidad y evita ambigüedad durante la ejecución.

Plantilla editable:

Elemento	Descripción
Objetivo de auditoría	
Criterios (ISO/Internos)	
Alcance (proceso/periodo)	
Métodos (doc/entrevista/obs.)	
Muestra seleccionada y justificación	
Equipo auditor	
Agenda y tiempos	

Sabías que:
Sin criterios explícitos, los hallazgos se vuelven opinables y pierden fuerza técnica.

Autoevaluación:
¿Tu plan permite a un tercero comprender exactamente qué será auditado y por qué?

Matriz Riesgo → Control → Evidencia → Hallazgo

Contenido principal (≤300):
Esta matriz conecta evaluación de riesgos con controles implementados y evidencia verificada. Permite al auditor demostrar trazabilidad lógica desde riesgo identificado hasta conclusión auditora, fortaleciendo defensa técnica del informe.

Plantilla editable:

Riesgo IA	Control Asociado	Evidencia Verificada	Cumple (S/N)	Hallazgo	Impacto/Riesgo Residual

Sabías que:
La trazabilidad evita hallazgos aislados y demuestra coherencia sistémica del SGIA.

Autoevaluación:
¿Puedes justificar cada hallazgo vinculándolo directamente con un riesgo identificado?

Checklist: Evidencia Suficiente y Apropiada

Contenido principal (≤300):
Antes de concluir, el auditor debe validar que la evidencia sea suficiente (cantidad)

y apropiada (relevante, verificable y confiable). Este checklist ayuda a evitar conclusiones débiles o basadas solo en declaraciones verbales.

Checklist verificable:

☐ ¿Existe criterio claramente definido?
☐ ¿La evidencia es verificable y trazable?
☐ ¿Se trianguló información (doc + entrevista + registro)?
☐ ¿La muestra está justificada por riesgo?
☐ ¿La evidencia cubre el periodo auditado?
☐ ¿Existe registro documentado en expediente?

Sabías que:
ISO 19011 establece que la evidencia debe ser verificable y generalmente basada en muestras.

Autoevaluación:
¿Cuál de estos puntos suele fallar con mayor frecuencia en tus auditorías?

Guía de Redacción de Hallazgos (Modelo + Ejemplo)

Contenido principal (≤300):
Un hallazgo sólido se estructura como: Criterio → Condición → Evidencia → Impacto → Conclusión. Esta guía evita subjetividad y facilita decisiones correctivas alineadas a riesgo.

Modelo estructural:

- **Criterio:** Cláusula 6.1 ISO 4200
- **Condición:** No se actualizó evaluación tras cambio de modelo
- **Evidencia:** Actas y matriz de riesgos versión 1.2 sin modificación
- **Impacto:** Riesgo residual no reevaluado
- **Conclusión:** No conformidad menor

Sabías que:
Separar claramente criterio y condición reduce discusiones y fortalece aceptación del hallazgo.

Autoevaluación:
¿Tu último hallazgo incluyó explícitamente el impacto en riesgo o solo describió la falla?

MÓDULO 6 — Mejora y Cierre (Cláusula 10)

Dom. D (C12, C13, C14)

6.1 Determinación de conformidad/NC/OM (3)

Conformidad vs NC vs OM con ejemplo rápido

Contenido principal (≤500):
Clasifica comparando evidencia verificable vs criterio. **NC** si el requisito no se cumple; **OM** si cumple, pero hay mejora sin incumplir. Micro-ejemplo: el control "revisión humana" exige registro. Si no hay registros en el periodo auditado → **NC**. Si hay registros, pero sin análisis de tendencias → **OM** (si el criterio no exige ese análisis).

Sabías que:
La clasificación incorrecta suele venir de no fijar el criterio exacto (norma/procedimiento) antes de mirar la evidencia.

Autoevaluación:
En tu organización, ¿qué caso típico se etiqueta como OM cuando en realidad es NC por falta de evidencia?

Criterio vs evidencia: mini-mapa de decisión

Contenido principal (≤500):
Primero fija el **criterio** (cláusula/política/procedimiento), luego verifica **evidencia** (registros, logs, actas). Mini-artefacto:

1. ¿Criterio exige “documentado”? → busca documento controlado.
2. ¿Exige “implementado”? → busca registros operativos.
3. ¿Exige “eficaz”? → busca métricas/resultado.
   Sin criterio o sin evidencia verificable, no hay hallazgo defendible.

Sabías que:
Muchas disputas se resuelven mostrando el “paso 1”: el criterio explícito y vigente.

Autoevaluación:
¿En qué parte fallas más: definir criterio, recolectar evidencia o conectar ambos en la redacción?

Severidad: regla práctica basada en riesgo

Contenido principal (≤500):
La severidad se justifica por **impacto + recurrencia + criticidad**. Micro-regla:

- **Mayor**: falla en control crítico o riesgo alto sin mitigación, evidencia de recurrencia o brecha sistémica.

- **Menor**: incumplimiento puntual con bajo impacto y sin recurrencia.
  Ejemplo: cambios de modelo sin aprobación en sistema IA de alto impacto → probable **NC mayor**.

Sabías que:
Una "falla documental" puede ser mayor si impide demostrar control en un proceso crítico.

Autoevaluación:
¿Qué evidencia te haría escalar una NC menor a mayor (recurrencia, impacto, o ambos)?

◇ 6.2 Hallazgos auditables (C13) (6)

▨ Hallazgo completo: plantilla mental + ejemplo

Contenido principal (≤500):
Estructura: **Criterio** → **Condición** → **Evidencia** → **Impacto** → **Conclusión**. Micro-ejemplo:
Criterio: procedimiento exige revisar sesgo mensual.
Condición: no se realizó revisión en 2 meses.
Evidencia: calendario sin entradas + ausencia de reportes.
Impacto: sesgo no detectado; riesgo residual aumenta.
Conclusión: NC (severidad según criticidad).

Sabías que:
Si falta impacto, el auditado no entiende urgencia; si falta evidencia, el hallazgo es discutible.

Autoevaluación:
¿Puedes escribir un hallazgo en 5 líneas siguiendo esa secuencia sin agregar opiniones?

Redacción objetiva: “verbo de evidencia”

Contenido principal (≤500):
Redacta con verbos verificables: “no existe”, “no se encontró”, “no hay registro”, “se observó”, “se evidenció”. Evita “malo/insuficiente”. Micro-ejemplo: en vez de “gestión débil de cambios”, escribe: “no se encontró acta de aprobación para cambios v3.2 (fecha X)”. Esto convierte debate en verificación.

Sabías que:
La objetividad mejora aceptación y reduce retrabajo del informe.

Autoevaluación:
Toma un hallazgo tuyo y reemplaza 2 adjetivos por evidencia concreta. ¿Qué cambia?

Evidencia suficiente/apropiada aplicada a IA

Contenido principal (≤500):
Para controles IA, evidencia típica: logs de monitoreo, tickets/incidentes, actas de cambios, SoA vigente, matriz de riesgos, reportes de métricas. Micro-artefacto de prueba:

- Entrevista dice “sí se revisa” → exige registro.
- Registro existe → valida periodo y completitud.
- Registro consistente → triangula con métricas o decisiones derivadas.

Sabías que:
La triangulación reduce el riesgo de “cumplimiento narrado”.

Autoevaluación:
¿En qué control IA sueles depender demasiado de entrevistas sin registros?

Comunicación de hallazgos: guion de 30 segundos

Contenido principal (≤500):
Comunica con un guion breve: **(1) criterio**, **(2) qué vimos**, **(3) evidencia**, **(4) impacto**, **(5) próximo paso**. Micro-ejemplo: "El procedimiento exige revisión mensual de deriva; en abril y mayo no hubo revisión (calendario vacío y sin reportes). Esto eleva riesgo de degradación no detectada. Recomendamos acción correctiva y verificación en 30 días".

Sabías que:
La claridad en cierre reduce "sorpresas" y mejora cooperación del auditado.

Autoevaluación:
¿Tu cierre deja claro qué debe hacer el auditado y qué evidencia se esperará después?

Priorización: matriz impacto × urgencia

Contenido principal (≤500):
Prioriza con matriz simple:

- Alto impacto + alta urgencia → atención inmediata (NC mayor probable).
- Alto impacto + baja urgencia → plan con fecha fija y control de riesgo.

- Bajo impacto + alta urgencia → corrección rápida.

- Bajo impacto + baja urgencia → OM o mejora planificada.
  Ejemplo: ausencia de supervisión humana en decisiones críticas → alto/alto.

Sabías que:
La priorización es parte del valor auditor: orienta recursos hacia reducción real de riesgo.

Autoevaluación:
¿Qué criterio usas hoy para definir plazos: riesgo o conveniencia operativa?

Consistencia informe: "regla de coherencia"

Contenido principal (≤500):
Regla: si hay **NC mayor** sin contención, no declares "SGIA eficaz". Alinea: hallazgos ↔ severidad ↔ conclusión global ↔ acciones requeridas. Micro-chequeo:

1. ¿Conclusión menciona debilidades críticas?

2. ¿Recomendaciones responden a causas?

3. ¿Seguimiento definido?
   Sin coherencia, el informe se percibe complaciente o incoherente.

Sabías que:
La coherencia protege al auditor ante revisión por dirección o auditoría externa.

Autoevaluación:
¿Has visto informes "positivos" con hallazgos críticos? ¿Qué riesgo genera eso?

◇ 6.3 Revisión por la dirección como insumo de mejora (C12) (4)

▨ Revisión por dirección: evidencia de gobierno

Contenido principal (≤500):
La revisión por dirección demuestra gobierno: evalúa si el SGIA sigue siendo adecuado al contexto y eficaz para controlar riesgos. Micro-evidencias: agenda, entradas analizadas (métricas, auditorías, NC, incidentes), decisiones registradas y asignación de recursos. El auditor verifica que la revisión use información crítica (sesgo/deriva/incidentes) y no solo reportes genéricos.

Sabías que:
Una reunión con acta sin decisiones no es evidencia fuerte de mejora.

Autoevaluación:
¿Qué entrada "no negociable" exigirías si el sistema IA impacta personas (equidad/seguridad)?

▨ Entradas obligatorias: mini-checklist de auditoría

Contenido principal (≤500):
Verifica entradas: resultados 9.1 (medición/análisis), 9.2 (auditorías), NC/AC, cambios en contexto/regulación, desempeño de proveedores, estado de riesgos y eficacia de controles. Micro-artefacto: marca "sí/no" por entrada y pide evidencia (documento, dashboard, acta). Si falta una entrada crítica, documenta el riesgo: decisiones basadas en información incompleta.

Sabías que:
Entradas incompletas suelen correlacionar con acciones correctivas ineficaces o tardías.

Autoevaluación:
¿Cuál entrada se omite más en tu organización: incidentes, proveedores o riesgos actualizados?

Salidas: decisiones accionables y medibles

Contenido principal (≤500):
Las salidas deben ser accionables: cambios en política/objetivos, recursos, controles, prioridades o aceptaciones de riesgo. Micro-ejemplo: "Aumentar cadencia de monitoreo de sesgo a semanal para sistema X; responsable Y; inicio fecha Z; KPI: % semanas con reporte". El auditor valida que cada salida tenga responsable, plazo y criterio de éxito.

Sabías que:
Una salida sin KPI o plazo se convierte en "intención" sin control.

Autoevaluación:
¿Qué evidencia pedirías para demostrar que una salida de dirección se implementó y funcionó?

Seguimiento: trazabilidad entrada→decisión→resultado

Contenido principal (≤500):
Audita el seguimiento: ¿las decisiones se ejecutaron?, ¿qué evidencia lo prueba?, ¿hubo verificación de eficacia? Micro-artefacto: traza 1 decisión de dirección hasta su evidencia: acta → ticket/plan → registro de implementación → métrica posterior. Si no hay seguimiento, la mejora continua es declarativa y los mismos temas reaparecen en auditorías sucesivas.

Sabías que:
Reincidencia es evidencia de que el sistema no aprende (o no controla).

Autoevaluación:
Elige una decisión de la última revisión: ¿puedes llegar a una métrica que demuestre su eficacia?

◇ 6.4 Acciones correctivas (C14) (6)

Corrección vs acción correctiva con ejemplo

Contenido principal (≤500):
Corrección = solución inmediata (contener). Acción correctiva = eliminar causa raíz y prevenir recurrencia. Micro-ejemplo: si falta registro de supervisión humana, corrección: crear registros para el mes en curso. Acción correctiva: ajustar proceso, roles, herramienta y control de cumplimiento para que el registro se genere siempre y se revise.

Sabías que:
Cerrar con "corrección" sin causa raíz explica la reincidencia en auditorías futuras.

Autoevaluación:
En tu experiencia, ¿qué se suele hacer más: correcciones rápidas o acciones correctivas reales?

Causa raíz: prueba de consistencia

Contenido principal (≤500):
Analiza causa raíz con método (5 porqués/Ishikawa). El auditor valida consistencia: ¿la causa explica el incumplimiento sin saltos? Micro-ejemplo: "no hay registros" → ¿por qué? "herramienta no obliga" → ¿por qué? "requisito no está en checklist" → causa probable: control de proceso incompleto. Evita causas vagas ("falta de cultura").

Sabías que:
Causas genéricas producen planes genéricos y resultados nulos.

Autoevaluación:
¿Tu organización documenta causas con evidencia o solo con declaraciones?

Plan de acción: calidad mínima esperada

Contenido principal (≤500):
Plan de acción debe incluir: acción específica, responsable, fecha, recurso, evidencia esperada y KPI de eficacia. Micro-ejemplo: "Implementar control automático de bloqueo si no hay revisión humana; dueño: Ops; fecha: 30 días; evidencia: logs de bloqueo; KPI: 100% decisiones críticas con revisión registrada". El auditor valida proporcionalidad vs riesgo.

Sabías que:
Planes sin KPI no permiten verificación de eficacia.

Autoevaluación:
¿Qué KPI usarías para una acción correctiva sobre deriva del modelo?

Implementación: evidencia mínima para "hecho"

Contenido principal (≤500):
Para confirmar implementación, exige evidencia verificable: configuración, procedimiento actualizado, capacitación aplicada, registros generados y control de cambios. Micro-artefacto: "paquete de cierre" con 3 piezas: (1) evidencia técnica (logs/config), (2) evidencia de proceso (procedimiento/roles), (3) evidencia de ejecución (registros del periodo). Sin paquete, no hay cierre sólido.

Sabías que:
Implementar “en palabra” es el origen de re-aperturas de NC.

Autoevaluación:
¿Qué evidencia pedirías si la acción correctiva es “capacitación” para asegurar que cambió la práctica?

Verificación de eficacia: prueba posterior

Contenido principal (≤500):
Verificar eficacia requiere evidencia **posterior** a la implementación: nueva medición, nuevo muestreo o auditoría de seguimiento. Micro-ejemplo: si la causa fue “cambios sin aprobación”, verifica 3 cambios posteriores: ¿hay acta?, ¿análisis de impacto?, ¿actualización de riesgos? Si la evidencia posterior no cambia, la acción no fue eficaz aunque esté “implementada”.

Sabías que:
Eficacia = prevención de recurrencia, no solo ejecución de tareas.

Autoevaluación:
¿Qué ventana temporal mínima usarías para verificar eficacia en un control operacional crítico?

Cierre formal de NC: criterio de cierre

Contenido principal (≤500):
Cierra una NC cuando: (1) corrección implementada, (2) causa raíz tratada, (3) eficacia verificada, (4) evidencias archivadas y trazadas al hallazgo. Micro-artefacto: registro de cierre con fecha, verificador, evidencia y resultado. Cierre prematuro se detecta por reincidencia o por ausencia de evidencia posterior.

Sabías que:
El cierre formal protege a la organización: documenta aprendizaje y control.

Autoevaluación:
¿Quién debería validar el cierre: el mismo responsable o un verificador independiente?

◇ 6.5 Cierre del curso (3)

▨ Checklist final del auditor (antes de emitir informe)

Contenido principal (≤500):
Checklist final: criterios citados, evidencias registradas, muestreo justificado, hallazgos completos (C-C-E-I-Concl), severidad justificada por riesgo, conflictos gestionados, acuerdos de cierre documentados y plan de seguimiento. Micro-uso: marca "OK/pendiente" para cada punto antes de enviar informe.

Sabías que:
Un checklist reduce omisiones que luego invalidan hallazgos o dificultan acciones correctivas.

Autoevaluación:
¿Qué punto del checklist te habría evitado un retrabajo reciente en un informe?

Estrategia tipo examen: método auditor en 3 pasos

Contenido principal (≤500):
En preguntas situacionales, aplica 3 pasos: (1) identifica el **criterio** implícito (cláusula/principio), (2) detecta la **evidencia disponible** y la que falta, (3) decide la **acción auditor** (hallazgo, severidad, evidencia adicional). Micro-ejemplo: "no hay registros" → pide evidencia; si criterio exige registro → NC.

Sabías que:
El examen premia lógica de auditoría: criterio + evidencia + juicio, más que memoria literal.

Autoevaluación:
¿Respondes primero por intuición o sigues un esquema criterio-evidencia-juicio?

Cierre: competencia del auditor SGIA

Contenido principal (≤500):
El auditor interno del SGIA aporta valor cuando conecta evidencia con riesgo y mejora: identifica fallas reales, comunica con claridad y verifica eficacia de acciones correctivas. Micro-compromiso: en tu próxima auditoría, selecciona 1 control crítico y demuestra su eficacia con evidencia posterior, no solo con documentación.

Sabías que:
La auditoría madura convierte hallazgos en aprendizaje organizacional medible.

Autoevaluación:
¿Cuál control crítico auditarás primero y qué evidencia posterior pedirás para probar eficacia?

ANEXO MÓDULO 6 — PLANTILLAS (NUEVAS SLIDES)

Plantilla: Clasificación de Hallazgos (NC Mayor/NC Menor/OM)

Contenido principal (≤500):
Usa esta plantilla para clasificar consistentemente: conecta criterio, evidencia y riesgo. Incluye recurrencia y criticidad para justificar severidad. Recomendada para estandarizar decisiones entre auditores y reducir subjetividad.

Plantilla editable (campos):

Criterio	Condición	Evidencia	Impacto	Recurrencia	Criticidad	Severidad propuesta	Justificación

Sabías que:
La severidad bien justificada acelera acciones proporcionales y reduce discusiones.

Autoevaluación:
¿Qué campo suele quedar débil en tus hallazgos: impacto, recurrencia o justificación?

▧ Plantilla: Registro de Hallazgos (C-C-E-I-Conclusión)

Contenido principal (≤500):
Estandariza redacción y trazabilidad: cada hallazgo debe poder reconstruirse desde evidencia hasta conclusión. Úsala como "unidad mínima" del informe para asegurar consistencia, claridad y alineación a criterios.

Plantilla editable:

Criterio (cláusula)	Condición (hecho)	Evidencia (qué/ dónde/ cuándo)	Impacto (riesgo)	Conclusión (NC/OM)

Sabías que:
Un registro uniforme facilita revisiones internas y auditorías de seguimiento.

Autoevaluación:
¿Tu evidencia incluye ubicación/versión/periodo para que sea verificable después?

▧ Plantilla: Acción Correctiva (Causa raíz → Plan → Implementación → Eficacia)

Contenido principal (≤500):
Esta plantilla asegura que la acción correctiva elimine causa raíz y se verifique su eficacia. Incluye KPI y evidencia posterior para evitar cierres prematuros. Útil para seguimiento y auditoría de eficacia.

Plantilla editable:

NC	Causa raíz	Acciones	Responsable	Fecha	Evidencia implementación	KPI eficacia	Resultado (eficaz/no)

Sabías que:
Sin KPI y evidencia posterior, no puede afirmarse prevención de recurrencia.

Autoevaluación:
¿Qué KPI elegirías para demostrar eficacia en "gestión de cambios del modelo"?

Checklist: Cierre de NC (verificación de eficacia)

Contenido principal (≤500):
Checklist para confirmar que la causa se eliminó y no solo el síntoma. Úsalo antes de cerrar formalmente una NC, especialmente en controles críticos o reincidentes.

Checklist verificable:
☐ Criterio citado y vigente
☐ Corrección aplicada (contención)
☐ Causa raíz documentada (método)
☐ Plan con responsables y fechas
☐ Evidencia de implementación (registros)
☐ Evidencia posterior (nuevo muestreo/medición)
☐ KPI de eficacia cumple
☐ Cierre validado por verificador independiente

Sabías que:
La evidencia posterior es lo que diferencia "tarea completada" de "riesgo reducido".

Autoevaluación:
¿Qué paso del checklist suele omitirse cuando hay presión por "cerrar rápido"?

AGENDA

Supuesto de diseño

- **Total recomendado: 140 slides** (nivel intermedio; incluye metodología ISO 19011, práctica de auditoría y evaluación de eficacia de controles).

- Distribución orientada por pesos JTA por dominio (aprox.):

    - **Dom. C (C8–C11): ~31% → 43 slides**
    - **Dom. B (C5–C7): ~26% → 36 slides**
    - **Dom. A (C1–C4): ~19% → 26 slides**
    - **Dom. D (C12–C14): ~15% → 22 slides**
    - **Dom. E (C15): ~9% → 13 slides**

Tabla de Contenido y Plan de Slides (I42001IA™)

Módulo 1 — Introducción y Contexto (Cláusulas 1–4)

Enfoque: Dom. E (C15) + ISO/IEC 22989 (terminología IA)
Objetivo auditor: entender el ecosistema IA y **definir alcance/auditabilidad** del

SGIA antes de auditar.
Slides sugeridas: 13

1.1 Propósito del curso y alcance del rol Internal Auditor (qué audita / qué no) (2)
1.2 Visión general ISO/IEC 42001: estructura HLS y lógica SGIA (2)
1.3 Terminología esencial para auditar IA (SGIA, sistema IA, ciclo de vida, impacto) (4)
1.4 Contexto organizacional y partes interesadas: qué evidencia buscar (3)
1.5 Determinación del alcance del SGIA: límites, interfaces, exclusiones justificadas (2)

Módulo 2 — Liderazgo y Planificación (Cláusulas 5–6)

Enfoque: Dom. C (C8, C9) + ISO/IEC 23894 (gestión de riesgos IA)
Objetivo auditor: verificar **coherencia política–objetivos–riesgo–SoA** y trazabilidad de decisiones.
Slides sugeridas: 22

2.1 Liderazgo en SGIA: responsabilidades, rendición de cuentas, gobierno (3)
2.2 Política de IA (C8): criterios de auditoría y evidencia típica (aprobación, comunicación, marco de objetivos) (5)
2.3 Objetivos de IA: consistencia, medición, planificación para lograrlos (3)
2.4 Planificación basada en riesgos: riesgos y oportunidades (2)
2.5 Evaluación de riesgos de IA (ISO 23894 como marco de referencia): entradas/salidas auditables (4)
2.6 Evaluación de impacto del sistema IA: cuándo aplica, evidencia y trazabilidad (3)
2.7 Tratamiento del riesgo y vínculo con controles + SoA (C9 introducción) (2)

Módulo 3 — Soporte y Operación (Cláusulas 7–8)

Enfoque: Dom. C (C10, C11) — Controles del Anexo A, SoA y eficacia en operación
Objetivo auditor: auditar **SoA**, determinar **aplicabilidad** y evaluar

diseño/operación/eficacia de controles con evidencia.
Slides sugeridas: 21 *(con esto Dom. C totaliza 43: M2(22)+M3(21))*

3.1 Soporte (7): competencia, concienciación, comunicación e información documentada como evidencia (5)
3.2 Operación (8): planificación y control operacional; cambios; procesos externalizados (4)
3.3 Anexo A: estructura de controles de referencia (qué es/qué no es) (3)
3.4 SoA en auditoría (C9): contenido mínimo, trazabilidad riesgo–control–justificación; errores comunes (4)
3.5 Determinar aplicabilidad de controles (C10): método y criterios; muestreo por criticidad/riesgo/ciclo de vida (3)
3.6 Evaluación de eficacia de controles (C11): "diseño vs operación vs resultado", evidencia suficiente y apropiada (2)

Módulo 4 — Evaluación del Desempeño (Cláusula 9)

Enfoque: Dom. B (C5, C6, C7)
Objetivo auditor: juzgar la **validez de métodos**, la ejecución en **intervalos planificados** y la **eficacia global** del SGIA integrando fuentes.
Slides sugeridas: 36

4.1 Qué evaluar: desempeño del SGIA vs desempeño del sistema IA (2)
4.2 9.1 Seguimiento y medición: qué medir, métodos válidos, frecuencia, registros (6)
4.3 Métricas específicas de IA para auditoría: precisión, sesgo, robustez, deriva, explicabilidad (8)
4.4 Validez/fiabilidad de métodos y datos (C5): evidencia, trazabilidad, dueños de métricas (6)
4.5 Verificación de intervalos planificados (C6): calendarios, evidencias, brechas y su impacto (5)
4.6 Integración para juicio de eficacia (C7): medición + auditorías + NC + revisión dirección (5)
4.7 9.3 Revisión por la dirección: entradas/salidas, evidencia y consistencia con riesgos/objetivos (4)

Módulo 5 — Auditoría Interna (ISO 19011 + 9.2 ISO/IEC 42001)

Enfoque: Dom. A (C1, C2, C3, C4)
Objetivo auditor: ejecutar auditorías internas del SGIA con **imparcialidad**, **criterios claros**, **muestreo** y **evidencia objetiva**.
Slides sugeridas: 26

5.1 Principios ISO 19011 aplicados a SGIA: integridad, presentación imparcial, debido cuidado, confidencialidad, independencia (4)
5.2 Programa de auditoría (C1): priorización por riesgo/cambios/resultados previos; recursos; plan anual (5)
5.3 Plan de auditoría (C2): objetivos, criterios, alcance, métodos, muestreo y plan de entrevistas (6)
5.4 Imparcialidad y conflictos (C3): evaluación, mitigación y evidencia documentada (4)
5.5 Obtención y registro de evidencia (C4): suficiencia/apropiación, triangulación, trazabilidad (5)
5.6 Taller tipo examen: mini-casos de evidencia (2)

Módulo 6 — Mejora y Cierre (Cláusula 10)

Enfoque: Dom. D (C12, C13, C14)
Objetivo auditor: formular hallazgos, verificar acciones correctivas y evidenciar mejora continua del SGIA.
Slides sugeridas: 22

6.1 Determinación de conformidad/NC/OM: criterios vs evidencia (3)
6.2 Hallazgos auditables (C13): estructura criterio–condición–evidencia; redacción; severidad; comunicación (6)
6.3 Revisión por la dirección como insumo de mejora (C12): evidencias, entradas obligatorias, seguimiento (4)
6.4 Acciones correctivas (C14): causa raíz, plan, implementación, verificación de eficacia (6)
6.5 Cierre del curso: checklist final del auditor + estrategia tipo examen (3)

Resumen de slides por módulo

- M1: 13
- M2: 22
- M3: 21
- M4: 36
- M5: 26
- M6: 22
  Total: 140 slides

Entregables didácticos recomendados (dentro de los módulos)

Para asegurar el foco “Internal Auditor” (evidencia y juicio):

- Plantilla de **Programa de Auditoría** (ISO 19011 / 9.2)
- Plantilla de **Plan de Auditoría** (objetivos/criterios/alcance/muestreo)
- Matriz de **trazabilidad Riesgo → Control → Evidencia → Hallazgo**
- Checklist de **suficiencia y apropiación** de evidencia
- Guía de redacción de hallazgos (**criterio–condición–evidencia–conclusión.**


certiprof®