ISO/IEC 42001

LEAD AUDITOR

PROFESSIONAL CERTIFICATION

certiprof®

I42001LA™ VERSIÓN 052026

Sistema de Gestión de Inteligencia Artificial

ISO/IEC 42001 — Formación para Auditores

Un marco organizacional para gobernar, controlar, evaluar y mejorar la forma en que los sistemas de IA son desarrollados, proporcionados o utilizados.

MÓDULO 1

Fundamentos del SGIA e ISO/IEC 42001

1. Introducción al Sistema de Gestión de IA

La inteligencia artificial se ha incorporado progresivamente en procesos de negocio, productos, servicios, decisiones operativas y actividades de soporte. Su adopción puede generar beneficios relevantes para las organizaciones, pero también introduce nuevos desafíos relacionados con el uso responsable, la supervisión humana, la calidad de los datos, la transparencia, la seguridad, la privacidad, la equidad, la rendición de cuentas y los impactos sobre personas, grupos u organizaciones.

> La gestión de la IA no puede limitarse al desempeño técnico de un modelo o a la adquisición de una herramienta tecnológica. Requiere un sistema organizacional capaz de **dirigir, controlar, evaluar y mejorar** la forma en que los sistemas de IA son desarrollados, proporcionados o utilizados.

ISO/IEC 42001 responde a esta necesidad mediante un enfoque de sistema de gestión. La norma proporciona una estructura para que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un Sistema de Gestión de Inteligencia Artificial dentro de su contexto. Su aplicación se enfoca en aquellas características propias de la IA que pueden requerir salvaguardas específicas, especialmente cuando los sistemas de IA tienen efectos relevantes sobre procesos, decisiones, partes interesadas o resultados organizacionales.

¿Qué es un SGIA?

Un Sistema de Gestión de Inteligencia Artificial, o **SGIA**, es el conjunto de elementos interrelacionados mediante los cuales una organización define políticas, objetivos, procesos, responsabilidades, controles, evidencias y mecanismos de mejora para gestionar sus sistemas de IA de manera responsable y alineada con sus objetivos.
En términos prácticos, el SGIA permite que la organización responda de forma estructurada a preguntas como:

- **¿Qué sistemas de IA están dentro del alcance?**
- **¿Para qué se usan o se desarrollan esos sistemas?**
- **¿Quién es responsable de su gestión, supervisión y desempeño?**
- **¿Qué riesgos de IA han sido identificados?**
- **¿Qué impactos pueden generarse sobre personas, grupos, clientes, usuarios, procesos o la sociedad?**
- **¿Qué controles se han seleccionado para tratar esos riesgos?**
- **¿Cómo se verifica si los controles son eficaces?**
- **¿Qué información documentada demuestra la conformidad y la mejora del sistema?**

El SGIA como gobierno organizacional

El SGIA no es un documento aislado ni una política general sobre IA. Es una forma de **gobierno organizacional** que integra dirección, planificación, operación, evaluación del desempeño y mejora continua. Por ello, debe conectarse con la estrategia, la cultura, los procesos, los recursos, los proveedores, las obligaciones aplicables y las expectativas de las partes interesadas.

Desde una perspectiva de auditoría, el SGIA es el **objeto principal de evaluación**. El auditor interno o líder no se limita a revisar si la organización usa IA, sino si la organización cuenta con un sistema de gestión capaz de controlar ese uso, demostrar evidencia objetiva, gestionar riesgos, evaluar impactos y mejorar de forma continua.

El esquema de certificación I42001IA™ define precisamente el rol auditor como la obtención y evaluación de evidencia objetiva para determinar si el SGIA es conforme con requisitos aplicables y si se implementa, mantiene y mejora eficazmente.

¿Para qué sirve un SGIA?

Un SGIA sirve para convertir el uso, desarrollo, provisión o supervisión de sistemas de IA en una práctica **gobernada, trazable y verificable**. Su propósito no es frenar la innovación, sino establecer las condiciones para que la IA pueda ser utilizada con mayor control, responsabilidad y confianza.

Función del SGIA	Explicación
Dirección y alineación	Permite conectar el uso de IA con la estrategia, los objetivos y las políticas de la organización.
Gobernanza	Define roles, responsabilidades, autoridades y mecanismos de rendición de cuentas.
Gestión de riesgos	Ayuda a identificar, evaluar, tratar y monitorear riesgos de IA según el contexto y el uso previsto.
Gestión de impactos	Permite analizar posibles consecuencias sobre individuos, grupos, organizaciones o la sociedad.
Control operacional	Establece procesos, criterios, controles y evidencia para operar sistemas de IA bajo condiciones definidas.
Transparencia y confianza	Favorece la comunicación adecuada con partes interesadas y la disponibilidad de información documentada.
Evaluación y mejora	Permite medir desempeño, auditar el sistema, revisar resultados y tomar acciones correctivas.

El valor del SGIA en contextos de alto impacto

El valor del SGIA se vuelve especialmente relevante cuando una organización utiliza IA en procesos de alto impacto, decisiones sensibles, automatización de actividades críticas, atención a clientes, análisis de datos personales, selección de personas, evaluación de riesgos, generación de contenido, seguridad, salud, educación, servicios financieros o relaciones con terceros.

⚠ Para el auditor, la utilidad del SGIA se observa en la capacidad de la organización para demostrar **trazabilidad**. Un sistema bien gestionado permite seguir la cadena entre contexto, partes interesadas, alcance, riesgos, impactos, controles, Declaración de Aplicabilidad, operación, medición, hallazgos y mejora.

Cuando esa cadena se rompe, aparecen brechas típicas de auditoría: controles sin justificación, riesgos sin tratamiento, responsabilidades ambiguas, evidencia insuficiente o decisiones de IA sin supervisión adecuada.

Diferencia entre sistema de IA y sistema de gestión de IA

Una distinción fundamental para el auditor es separar el **sistema de IA** del **Sistema de Gestión de IA**.

Sistema de IA

Sistema basado en máquinas que, a partir de entradas, genera salidas como predicciones, recomendaciones, contenido o decisiones apoyadas por IA.

Debe usarse "sistema de IA" en lugar de expresiones ambiguas como "herramienta inteligente" o formulaciones que atribuyan capacidades humanas al sistema.

Sistema de Gestión de IA

Marco organizacional que dirige y controla cómo esos sistemas de IA son gobernados, evaluados, utilizados, monitoreados y mejorados.

Es el conjunto de políticas, procesos, responsabilidades y controles que permiten gobernar la IA de forma estructurada.

Comparación detallada

Aspecto	Sistema de IA	Sistema de Gestión de IA
Naturaleza	Sistema tecnológico o sociotécnico que produce salidas de IA.	Sistema organizacional de gestión, gobierno y control.
Función principal	Generar predicciones, recomendaciones, contenido, clasificaciones o apoyo a decisiones.	Establecer políticas, objetivos, procesos, responsabilidades, controles y mejora.
Ejemplos	Modelo de clasificación, sistema de recomendación, IA generativa, sistema predictivo.	Política de IA, evaluación de riesgos, evaluación de impacto, SoA, auditoría, revisión por la dirección.
Responsabilidad	Puede involucrar equipos técnicos, proveedores, usuarios y dueños de proceso.	Recae en la organización, la alta dirección y los roles definidos dentro del SGIA.
Evidencia típica	Registros de desempeño, datos utilizados, pruebas, monitoreo técnico, salidas generadas.	Alcance, política, objetivos, análisis de riesgos, controles, información documentada, auditorías y acciones correctivas.
Pregunta auditora	¿El sistema funciona dentro de parámetros definidos?	¿La organización gobierna, controla, evalúa y mejora la IA de forma conforme y eficaz?

Error común en auditoría

Esta diferencia evita un error común: **auditar únicamente el desempeño técnico del sistema de IA** y concluir que el SGIA es eficaz. Un sistema de IA puede mostrar resultados técnicamente aceptables y, aun así, estar mal gobernado si no existen responsabilidades claras, controles aplicables, evaluación de impacto, monitoreo de riesgos, información documentada o mecanismos de mejora.

De igual forma, un SGIA no se limita a documentar políticas. Debe demostrar que las políticas, objetivos, controles y procesos se aplican sobre sistemas de IA reales dentro del alcance definido.

Estructura de gestión

Políticas, roles, responsabilidades, controles y procesos definidos.

Aplicación práctica

Implementación real sobre sistemas de IA dentro del alcance con evidencia objetiva.

La auditoría del SGIA requiere revisar **tanto** la estructura de gestión **como** su aplicación práctica.

Rol de ISO/IEC 42001 en la gobernanza de IA

ISO/IEC 42001 proporciona un marco internacional para estructurar la gobernanza de IA desde la lógica de los sistemas de gestión. Su valor está en permitir que organizaciones de distinto tamaño, sector y naturaleza puedan establecer un enfoque sistemático para gestionar sistemas de IA dentro de su contexto. La adopción de un sistema de gestión de IA es una decisión estratégica influida por necesidades, objetivos, procesos, tamaño, estructura y expectativas de partes interesadas. La aplicación puede realizarse mediante un **enfoque basado en riesgos**, con controles proporcionales a los casos de uso, servicios o productos de IA dentro del alcance.

En gobernanza de IA, ISO/IEC 42001 cumple cuatro funciones principales.

01

Ordena la responsabilidad organizacional

La gobernanza de IA involucra alta dirección, responsables de procesos, áreas legales, cumplimiento, seguridad, privacidad, gestión de riesgos, proveedores, usuarios y otras partes interesadas. La norma ayuda a ubicar esas responsabilidades dentro de un sistema formal.

02

Conecta la IA con el enfoque basado en riesgos

La organización debe comprender su contexto, identificar riesgos de IA, evaluar impactos, seleccionar controles y revisar si las acciones implementadas son eficaces.

03

Introduce evidencia y trazabilidad

Un SGIA debe apoyarse en información documentada, registros, decisiones justificadas, criterios de evaluación, controles seleccionados y resultados medibles.

04

Facilita la mejora continua

El SGIA debe monitorearse, auditarse, revisarse por la dirección y mejorarse cuando existan cambios, no conformidades, nuevos riesgos, resultados insuficientes o ajustes en el contexto.

ISO/IEC 42001 e ISO 19011 en auditoría

ISO/IEC 42001

Actúa como **criterio principal** para evaluar el SGIA. Define los requisitos que la organización debe cumplir en materia de gobernanza de IA.

ISO 19011

Orienta la **metodología de auditoría**. Proporciona directrices para planificar, ejecutar y reportar auditorías de sistemas de gestión.

El documento de alcance de I42001IA™ confirma que el rol se centra en **aseguramiento y auditoría con evidencia**, no en habilidades de ingeniería o entrenamiento de modelos. Vincula el ciclo de auditoría con programa, planificación, imparcialidad, evidencia, evaluación del desempeño, controles/SoA, hallazgos, acción correctiva y mejora.

Enfoque para el auditor

Para un auditor, este primer tema debe dejar una idea central: **ISO/IEC 42001 no se audita como una lista de documentos, sino como un sistema de gestión aplicado a sistemas de IA concretos.**

Pregunta clave	Propósito auditor
¿Qué sistemas de IA están dentro del alcance?	Confirmar que el SGIA cubre los usos, procesos o servicios relevantes.
¿Qué rol cumple la organización frente a esos sistemas?	Entender responsabilidades como usuaria, proveedora, desarrolladora, integradora u operadora.
¿Qué riesgos de IA han sido identificados?	Revisar si el enfoque basado en riesgos es real y contextualizado.
¿Qué impactos se han evaluado?	Verificar consecuencias potenciales sobre personas, grupos, organización o sociedad.
¿Qué controles se han seleccionado?	Evaluar coherencia entre riesgo, tratamiento, Anexo A y SoA.
¿Qué evidencia demuestra implementación y eficacia?	Sustentar conclusiones de conformidad, no conformidad o mejora.
¿Cómo se revisa y mejora el SGIA?	Confirmar que el sistema no es estático y que aprende organizacionalmente mediante revisión, auditoría y acción correctiva.

La competencia del auditor no consiste en reemplazar al especialista técnico de IA, sino en evaluar si la organización cuenta con un sistema de gestión capaz de gobernar la IA con criterios definidos, responsabilidades claras, controles proporcionados, evidencia objetiva y mejora continua.

Estructura de ISO/IEC 42001

ISO/IEC 42001 sigue la lógica de los sistemas de gestión ISO. Esto significa que no está diseñada como una guía técnica para construir modelos de IA, sino como un marco para **establecer, implementar, mantener y mejorar** un Sistema de Gestión de Inteligencia Artificial dentro de una organización.

Para un auditor, comprender la estructura de ISO/IEC 42001 es fundamental porque cada sección cumple una función dentro del sistema. Las cláusulas iniciales delimitan el alcance, las referencias y los términos. Las cláusulas 4 a 10 contienen los requisitos principales del SGIA. Los anexos complementan la norma mediante controles de referencia, orientación para su implementación y elementos de contexto para analizar objetivos, riesgos y aplicación sectorial.

La auditoría de un SGIA no consiste en revisar la norma de forma aislada, sino en comprender cómo sus requisitos se conectan entre sí: contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Esta conexión permite evaluar si la organización gobierna sus sistemas de IA de manera coherente, trazable y eficaz.

Alcance general de ISO/IEC 42001

ISO/IEC 42001 establece requisitos para un Sistema de Gestión de Inteligencia Artificial. Su propósito es ayudar a las organizaciones a gestionar sistemas de IA de forma responsable, considerando su contexto, sus objetivos, sus riesgos, sus impactos y las expectativas de las partes interesadas.

La norma puede aplicarse a organizaciones de distintos tamaños, sectores y niveles de madurez. También puede ser utilizada por organizaciones que **desarrollan, proveen, integran, adquieren o utilizan** sistemas de IA.

Una organización que usa un sistema de IA de un proveedor externo también necesita definir responsabilidades, controles, supervisión y evidencia. La responsabilidad frente a la IA no se limita a quienes crean modelos o algoritmos.

Desde la perspectiva del auditor, el alcance general de ISO/IEC 42001 permite formular una primera pregunta clave:

¿La organización ha definido un SGIA que corresponde realmente a sus sistemas de IA, a su rol frente a esos sistemas y a los riesgos e impactos asociados?

Evaluación del alcance en auditoría

La respuesta a la pregunta sobre el alcance no se obtiene solo revisando una declaración de alcance. El auditor debe analizar si el alcance del SGIA refleja la realidad operativa de la organización. Para ello, puede revisar información sobre procesos, productos, servicios, unidades organizacionales, sistemas de IA, proveedores, usuarios, partes interesadas y obligaciones aplicables.

⚠ Un alcance débil o ambiguo puede limitar la utilidad del SGIA. Por ejemplo, una organización podría declarar que su SGIA cubre “el uso de IA en la empresa”, pero no identificar qué sistemas de IA están incluidos, qué procesos los utilizan, quién los supervisa o qué proveedores participan. En ese caso, el auditor tendría una señal de alerta: el alcance no permite verificar con claridad la conformidad ni la eficacia del sistema.

Características de un alcance bien definido

Por el contrario, un alcance bien definido permite entender:

- **Qué sistemas de IA están cubiertos**
- **Qué procesos, áreas o servicios están incluidos**
- **Qué límites y exclusiones existen y por qué**
- **Qué partes interesadas son relevantes**
- **Qué riesgos e impactos deben considerarse**
- **Qué controles aplican dentro del SGIA**

En síntesis, el alcance general de ISO/IEC 42001 ubica a la organización frente a la responsabilidad de gobernar la IA como parte de un sistema de gestión, no como una actividad técnica aislada.

Cláusulas 4 a 10

Las cláusulas 4 a 10 constituyen el cuerpo principal de requisitos del SGIA. Estas cláusulas siguen la estructura común de los sistemas de gestión ISO y permiten organizar el sistema desde la comprensión del contexto hasta la mejora continua.

Para el auditor, estas cláusulas deben leerse como una **secuencia lógica**. Cada una responde a una pregunta esencial sobre la gestión de la IA.

Cada cláusula cumple una función específica dentro del sistema y se conecta con las demás para garantizar coherencia, trazabilidad y eficacia del SGIA.

CLÁUSULA 4

Contexto de la organización

La cláusula 4 orienta a la organización a comprender el entorno en el que opera y a determinar el alcance del SGIA. Esto incluye analizar cuestiones internas y externas, partes interesadas, requisitos aplicables, límites del sistema y procesos necesarios.

Para el auditor, esta cláusula permite evaluar si el SGIA parte de una comprensión realista del contexto. No basta con que exista un documento de contexto; debe existir **coherencia** entre el contexto identificado, los sistemas de IA incluidos, las partes interesadas, los riesgos, los impactos y el alcance definido.

CLÁUSULA 5

Liderazgo

La cláusula 5 aborda el compromiso de la alta dirección, la política de IA y la asignación de roles, responsabilidades y autoridades. En un SGIA, el liderazgo es clave porque la gobernanza de IA requiere decisiones organizacionales, asignación de recursos y rendición de cuentas.

⚠ Para el auditor, esta cláusula permite revisar si la dirección del SGIA está respaldada por decisiones reales. Una política de IA aprobada no es suficiente si no se comunica, no se integra en procesos, no orienta objetivos o no se refleja en responsabilidades claras.

Planificación

La cláusula 6 se centra en la planificación del SGIA. Incluye acciones para abordar riesgos y oportunidades, evaluación de riesgos de IA, tratamiento del riesgo, evaluación de impacto del sistema de IA, objetivos de IA y planificación de cambios.

Para el auditor, esta cláusula es una de las más importantes porque **conecta la intención de gobierno con decisiones verificables**. La organización debe demostrar que los riesgos e impactos de IA han sido considerados y que existen acciones planificadas para tratarlos.

CLÁUSULA 7

Soporte

La cláusula 7 reúne los elementos de soporte necesarios para que el SGIA funcione: recursos, competencia, toma de conciencia, comunicación e información documentada.

Recursos
Humanos, tecnológicos y financieros necesarios para operar el SGIA.

Competencia
Habilidades y conocimientos requeridos para los roles dentro del SGIA.

Comunicación
Mecanismos internos y externos para transmitir información relevante del SGIA.

Información documentada
Registros, políticas, procedimientos y evidencias que respaldan el sistema.

Para el auditor, esta cláusula permite revisar si la organización cuenta con las condiciones necesarias para implementar y mantener el SGIA. Un sistema de gestión puede estar bien diseñado, pero fallar si no existen recursos, competencias o comunicación suficiente.

CLÁUSULA 8

Operación

La cláusula 8 se enfoca en la planificación y control operacional. Aquí se verifica cómo la organización lleva a la práctica lo que planificó en el SGIA. Incluye la ejecución de procesos, la implementación de controles, el tratamiento de riesgos y la gestión operativa de aspectos relacionados con sistemas de IA.

> Para el auditor, esta cláusula permite pasar de la revisión documental a la revisión de implementación. La pregunta central es: **¿La organización opera el SGIA de acuerdo con lo planificado y conserva evidencia de ello?**

CLÁUSULA 9

Evaluación del desempeño

La cláusula 9 aborda seguimiento, medición, análisis, evaluación, auditoría interna y revisión por la dirección. Su función es comprobar si el SGIA funciona y si produce los resultados previstos.

Seguimiento y medición

¿Se asegura la organización mide lo correcto, con métodos válidos, en intervalos adecuados y con evidencia suficiente?

Auditoría interna

¿Se realizan auditorías planificadas con criterios, alcance y metodología definidos?

Revisión por la dirección

¿Los resultados se analizan y se utilizan para tomar decisiones organizacionales?

CLÁUSULA 10

Mejora

La cláusula 10 se centra en la mejora continua, la gestión de no conformidades y las acciones correctivas. En un SGIA, la mejora es esencial porque los sistemas de IA, los datos, los usos, los proveedores, el contexto regulatorio y los impactos pueden cambiar con el tiempo.

Para el auditor, esta cláusula permite revisar si la organización **aprende de sus resultados**. Una no conformidad no debe cerrarse únicamente con una corrección inmediata. Debe analizarse la causa, definir acciones correctivas, implementarlas y verificar su eficacia.

Relación con el ciclo PHVA

ISO/IEC 42001 puede entenderse mediante el ciclo PHVA: **Planificar, Hacer, Verificar y Actuar**. Este ciclo permite organizar el SGIA como un sistema dinámico que se planifica, se implementa, se evalúa y se mejora.

Ciclo PHVA	Cláusulas relacionadas	Enfoque dentro del SGIA
Planificar	Cláusulas 4, 5 y 6	Comprender el contexto, definir liderazgo, política, roles, riesgos, impactos, objetivos y planes.
Hacer	Cláusulas 7 y 8	Proporcionar recursos, competencias, comunicación, información documentada y ejecutar los procesos operativos del SGIA.
Verificar	Cláusula 9	Medir, analizar, evaluar, auditar internamente y revisar el SGIA por la dirección.
Actuar	Cláusula 10	Corregir no conformidades, ejecutar acciones correctivas y mejorar continuamente el SGIA.

El ciclo PHVA desde la perspectiva auditora

1. Planificar

El auditor revisa si la organización comprende su contexto, define un alcance adecuado, asigna responsabilidades, identifica riesgos de IA, evalúa impactos y establece objetivos.

2. Hacer

El auditor verifica si la organización implementa lo planificado: recursos, controles, procesos, comunicación, información documentada y operación controlada de los sistemas de IA.

3. Verificar

El auditor analiza si la organización mide el desempeño del SGIA, revisa la eficacia de controles, realiza auditorías internas y lleva los resultados a la revisión por la dirección.

4. Actuar

El auditor evalúa si la organización responde a no conformidades, ejecuta acciones correctivas, verifica eficacia y utiliza la información obtenida para mejorar el SGIA.

Desconexiones típicas en el ciclo PHVA

El ciclo PHVA evita que el SGIA se convierta en un conjunto de documentos estáticos. También permite al auditor identificar desconexiones:

Riesgos sin controles

Riesgos identificados que no tienen controles asociados.

Controles no implementados

Controles definidos que no se aplican en la operación real.

Indicadores sin análisis

Indicadores que no se analizan ni se utilizan para tomar decisiones.

Hallazgos sin acción

Auditorías que generan hallazgos sin acciones correctivas asociadas.

Acciones sin evidencia

Acciones correctivas cerradas sin evidencia de eficacia.

Revisión sin seguimiento

Revisión por la dirección sin decisiones o seguimiento documentado.

Cuando el ciclo PHVA funciona correctamente, la organización puede demostrar que la gobernanza de IA no depende de acciones aisladas, sino de un sistema que aprende, se ajusta y mejora de manera continua.

Términos esenciales

La auditoría de un Sistema de Gestión de Inteligencia Artificial requiere **precisión terminológica**. En ISO/IEC 42001, los términos no se usan solo para describir tecnología; también permiten delimitar responsabilidades, criterios, evidencia, hallazgos y acciones de mejora.

Un auditor debe emplear los términos de forma consistente, **evitando expresiones ambiguas o antropomórficas** que atribuyan al sistema de IA capacidades humanas como intención, comprensión, pensamiento o juicio propio.

Términos fundamentales del SGIA

3.1 Sistema de IA

Sistema basado en máquinas que procesa entradas y genera salidas como predicciones, recomendaciones, contenido, clasificaciones o apoyo a decisiones. Para el auditor, identificar correctamente los sistemas de IA dentro del alcance es el primer paso para determinar qué procesos, datos, riesgos, controles, proveedores y partes interesadas deben revisarse.

3.2 SGIA

Conjunto de políticas, objetivos, procesos, responsabilidades, controles, información documentada y mecanismos de mejora mediante los cuales una organización gestiona sus sistemas de IA. El SGIA es el objeto principal de evaluación en auditoría.

3.3 Riesgo de IA

Efecto de la incertidumbre asociado al uso, desarrollo, integración, provisión o supervisión de sistemas de IA. Puede relacionarse con impactos técnicos, operativos, legales, éticos, sociales, reputacionales, de privacidad, seguridad, equidad o transparencia. No todo riesgo de IA es exclusivamente tecnológico.

Evaluación de impacto, política y objetivos

3.4 Evaluación de impacto del sistema de IA

Proceso mediante el cual la organización identifica y analiza posibles consecuencias del sistema de IA sobre individuos, grupos, organizaciones o la sociedad. Complementa la gestión de riesgos, pero no debe confundirse con ella: la gestión de riesgos se enfoca en la incertidumbre; la evaluación de impacto analiza consecuencias potenciales o reales.

3.5 Política de IA

Expresa la dirección y los compromisos de la organización respecto al uso, desarrollo, provisión o gestión de sistemas de IA. Debe estar alineada con el propósito organizacional, el contexto, los objetivos del SGIA y los requisitos aplicables. No debe ser solo una declaración aspiracional.

3.6 Objetivos de IA

Resultados que la organización busca alcanzar en relación con su SGIA. Deben ser coherentes con la política de IA, pertinentes para las funciones y niveles aplicables, y estar sujetos a seguimiento. Pueden relacionarse con gobernanza, reducción de riesgos, calidad de datos, supervisión humana, transparencia o cumplimiento.

3.7 Información documentada

La información documentada es la información que la organización debe controlar y mantener como soporte del SGIA. Puede incluir políticas, procedimientos, registros, evaluaciones, planes, informes, evidencias de auditoría, revisiones, resultados de medición y acciones correctivas.

En auditoría, la información documentada permite demostrar que las actividades del SGIA no solo fueron declaradas, sino **planificadas, ejecutadas, revisadas y mejoradas**.

El auditor debe verificar que la información documentada sea:

- **Identificable**
  Con referencia, versión y fecha clara.
- **Actualizada**
  Vigente y coherente con el estado actual del SGIA.
- **Protegida**
  Con controles de acceso y resguardo adecuados.
- **Disponible**
  Accesible para quienes la necesitan en el momento oportuno.
- **Controlada frente a cambios**
  Con mecanismos de revisión y aprobación de modificaciones.
- **Trazable**
  Vinculada al requisito o proceso que respalda.
- **Suficiente**
  Capaz de sustentar conclusiones de auditoría.

3.8 Conformidad, no conformidad y acción correctiva

Conformidad

Cumplimiento de un requisito. En una auditoría del SGIA, puede referirse al cumplimiento de ISO/IEC 42001, requisitos internos, requisitos legales, contractuales, controles definidos o criterios establecidos por la organización.

No conformidad

Incumplimiento de un requisito. No debe formularse como una opinión general ni como una preferencia del auditor. Debe estar respaldada por un criterio claro y evidencia objetiva.

Acción correctiva

Acción orientada a eliminar la causa de una no conformidad y prevenir su recurrencia. No debe confundirse con una corrección inmediata. Corregir resuelve el problema detectado; la acción correctiva aborda la causa que permitió que el problema ocurriera.

Aplicación práctica de los conceptos

Concepto	Enfoque	Pregunta clave para el auditor
Conformidad	Cumplimiento demostrado	¿La evidencia prueba que el requisito se cumple?
No conformidad	Incumplimiento evidenciado	¿Qué requisito no se cumple y qué evidencia lo demuestra?
Acción correctiva	Eliminación de causa	¿La organización trató la causa y verificó eficacia?

El uso correcto de estos términos permite que los hallazgos sean claros, trazables y defendibles. En una auditoría del SGIA, una conclusión sólida siempre conecta tres elementos: **criterio, evidencia y juicio auditor**.

Lectura auditora de la norma

> Auditar ISO/IEC 42001 no consiste en repetir el texto de la norma ni en verificar documentos de forma mecánica. Consiste en **interpretar cada requisito como un criterio de auditoría**, obtener evidencia objetiva y determinar si el SGIA demuestra conformidad, implementación y eficacia.

Convertir una cláusula en criterio de auditoría

Una cláusula se convierte en criterio cuando el auditor la utiliza como referencia para comparar lo que la organización ha definido, implementado y documentado.

Elemento	Pregunta guía
Cláusula	¿Qué aspecto del SGIA regula?
Criterio	¿Qué condición debe cumplirse?
Evidencia	¿Qué información demuestra cumplimiento?
Juicio auditor	¿La evidencia es suficiente para concluir conformidad?

Por ejemplo, si una cláusula trata sobre competencia, el auditor no debería limitarse a preguntar si existe capacitación. Debe verificar si la organización identificó las competencias necesarias, si las personas son competentes para sus roles dentro del SGIA y si existe información documentada que lo demuestre.

Diferenciar requisito, evidencia y hallazgo

Una auditoría sólida distingue claramente tres conceptos:

Concepto	Significado
Requisito	Lo que debe cumplirse según la norma, la organización o una obligación aplicable.
Evidencia	Información verificable que demuestra lo que ocurre en la práctica.
Hallazgo	Resultado de comparar la evidencia contra el criterio de auditoría.

Ejemplo práctico: requisito, evidencia y hallazgo

Un hallazgo no debe basarse en opiniones, suposiciones o preferencias del auditor. Debe vincularse con un criterio específico y con evidencia objetiva.

01

Requisito

La organización debe conservar información documentada sobre una actividad del SGIA.

02

Evidencia

Registros disponibles, controlados y trazables que demuestran la ejecución de la actividad.

03

Hallazgo

Conformidad si los registros existen y son adecuados. **No conformidad** si la información requerida no está disponible, no es trazable o no demuestra ejecución.

Evitar auditar solo documentos

La documentación es importante, pero no es suficiente. Un SGIA puede tener políticas, procedimientos y matrices completas, y aun así no estar implementado eficazmente.

El auditor debe revisar tres niveles:

Nivel	Qué verifica
Diseño	El proceso, control o política está definido.
Implementación	Se aplica en la operación real.
Eficacia	Produce el resultado esperado y contribuye al control del riesgo.

Por ejemplo, una SoA puede declarar que un control es aplicable, pero el auditor debe verificar si ese control está implementado, si existe evidencia de ejecución y si realmente contribuye a tratar el riesgo de IA asociado.

MÓDULO 2

Diseño, gobierno e implementación del SGIA

Introducción al Módulo

En este módulo se desarrolla la parte central del Sistema de Gestión de Inteligencia Artificial (SGIA), conforme a la estructura de requisitos de ISO/IEC 42001 desde la cláusula 4 hasta la cláusula 8. Estas cláusulas constituyen el núcleo de diseño, gobierno, planificación, soporte y ejecución del sistema.

> Para un auditor, este módulo es esencial porque aquí se concentra la mayor parte de los criterios que permiten verificar si una organización ha establecido un SGIA de forma coherente, si lo ha implementado en la práctica y si mantiene evidencia objetiva de su funcionamiento.

A diferencia de una lectura puramente técnica, el enfoque auditor exige revisar cómo se integran contexto, liderazgo, responsabilidades, riesgos, impactos, objetivos, recursos, competencia, comunicación, información documentada y operación del SGIA. No se trata de evaluar únicamente si existe documentación, sino si la organización demuestra que el sistema funciona y está alineado con sus sistemas de IA, su contexto y sus objetivos.

Contexto de la organización

Comprensión de la organización y de su contexto

La subcláusula 4.1 exige que la organización determine las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos del SGIA.

Cuestiones externas

Factores regulatorios, tecnológicos, económicos, contractuales, sociales, culturales o sectoriales que inciden sobre la forma en que la organización desarrolla, provee o utiliza sistemas de IA.

Cuestiones internas

Estructura organizacional, funciones, procesos, recursos, cultura, nivel de madurez, capacidades técnicas, relaciones con proveedores, criterios de gobernanza y mecanismos de control existentes.

Contexto específico para sistemas de IA

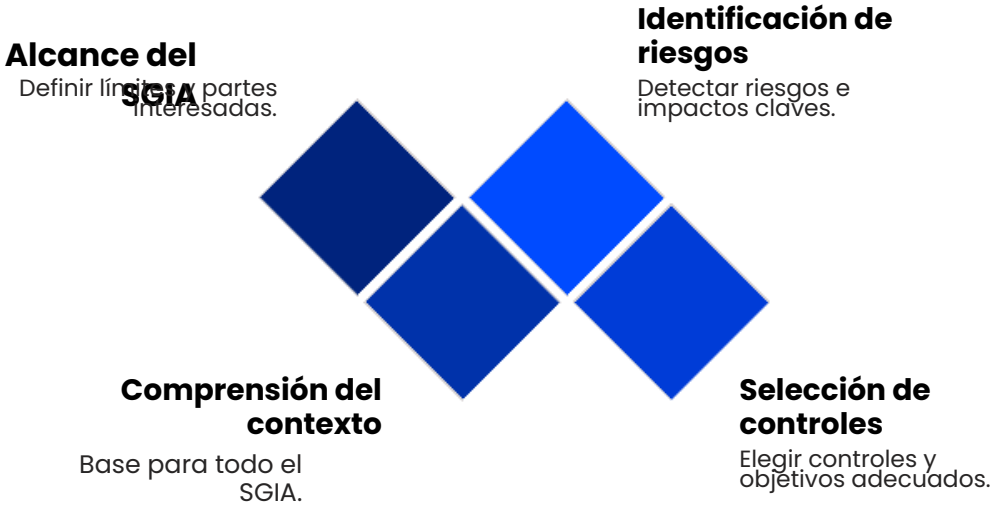
En un SGIA, el contexto no se define en abstracto. Se analiza específicamente en relación con los sistemas de IA dentro del alcance, su propósito previsto, las decisiones que apoyan o automatizan, los datos que utilizan, las partes interesadas involucradas y los posibles riesgos o impactos asociados.

Ejemplos de cuestiones que pueden considerarse:

- **Marco legal aplicable al uso de IA**
- **Dependencia de proveedores externos de tecnología o datos**
- **Expectativas del sector en materia de responsabilidad y transparencia**
- **Nivel de supervisión humana requerida**
- **Uso de sistemas de IA en decisiones sensibles**
- **Madurez de la organización para gestionar riesgos de IA**

El contexto como base del

⚠ La comprensión del contexto sirve como base para casi todo el SGIA: determinar el alcance, identificar partes interesadas, evaluar riesgos, analizar impactos, seleccionar controles, definir objetivos y planificar acciones. Por ello, en auditoría, **una falla en el análisis de contexto suele reflejarse posteriormente en inconsistencias del sistema completo**.



El auditor debe verificar que el análisis de contexto sea real, actualizado y coherente con los sistemas de IA incluidos en el alcance del SGIA.

Comprensión de las partes interesadas

La subcláusula 4.2 requiere que la organización determine las partes interesadas pertinentes para el SGIA y los requisitos relevantes de dichas partes interesadas.

Partes interesadas típicas

- Clientes y usuarios de sistemas de IA
- Personas o grupos afectados por salidas de IA
- Alta dirección y empleados internos
- Proveedores y socios tecnológicos
- Autoridades regulatorias
- Organismos de certificación
- Sociedad en general

Requisitos relevantes

- Leyes y reglamentos aplicables
- Contratos y estándares
- Políticas internas
- Compromisos de transparencia
- Condiciones de seguridad y privacidad
- Criterios éticos
- Expectativas de supervisión humana

Valor de identificar partes interesadas

Esta subcláusula permite que el SGIA no se limite a la perspectiva interna de la organización. También incorpora las necesidades, expectativas y requisitos de quienes pueden afectar o verse afectados por el uso, desarrollo, provisión o integración de sistemas de IA.

Una identificación adecuada de partes interesadas ayuda a definir mejor el **alcance, los riesgos, los controles, la comunicación y la información documentada** requerida por el SGIA.

Determinación del alcance del SGIA

La subcláusula 4.3 requiere que la organización determine los límites y la aplicabilidad del SGIA para establecer su alcance. Al determinarlo, la organización debe considerar:

01

Cuestiones internas y externas (4.1)

El entorno en el que opera la organización y los factores que afectan su capacidad de gestionar IA.

02

Requisitos de partes interesadas (4.2)

Las necesidades, expectativas y obligaciones de quienes se relacionan con los sistemas de IA.

03

Sistemas de IA y contextos de uso

Los sistemas de IA relacionados con las actividades de la organización y su propósito previsto.

En la práctica, el alcance debe indicar de forma suficientemente clara qué parte de la organización, qué funciones, qué procesos, qué servicios o qué sistemas de IA están cubiertos por el SGIA.

Preguntas clave sobre el alcance

¿Qué sistemas de IA están incluidos?

¿La organización actúa como desarrolladora, proveedora, integradora o usuaria?

¿Qué ubicaciones, áreas o unidades organizacionales participan?

¿Qué actividades o procesos están dentro y fuera del SGIA?

¿Qué exclusiones existen y cuál es su justificación?

El alcance puede ser amplio o específico, pero siempre debe ser coherente con el propósito del SGIA y con la realidad operacional. Un alcance demasiado general puede dificultar la auditoría; uno demasiado limitado puede dejar fuera riesgos o impactos relevantes. En auditoría, el alcance constituye un **punto crítico** porque condiciona todos los criterios de evaluación posteriores.

Sistema de Gestión de IA

La subcláusula 4.4 exige que la organización **establezca, implemente, mantenga y mejore continuamente** un SGIA, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de la norma.
Esta subcláusula integra lo definido en 4.1, 4.2 y 4.3, y convierte esos elementos en un sistema de gestión operable. No basta con identificar contexto, partes interesadas y alcance; la organización debe estructurar procesos y mecanismos concretos para gobernar sus sistemas de IA.

Para auditoría, esta subcláusula es la **afirmación central del sistema**: la organización no solo declara intenciones, sino que ha establecido un SGIA que funciona como sistema de gestión.

Procesos interrelacionados del SGIA

La subcláusula 4.4 también implica identificar cómo se relacionan entre sí los procesos del SGIA:

CLÁUSULA 5

Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al SGIA. En ISO/IEC 42001, esto significa que no puede delegar totalmente la gobernanza de IA en áreas técnicas o de cumplimiento, sino que debe asumir **responsabilidad activa** sobre la dirección, integración y eficacia del sistema.

Compatibilidad estratégica

Asegurar que la política y los objetivos de IA sean compatibles con la dirección estratégica de la organización.

Integración en procesos

Integrar los requisitos del SGIA en los procesos de negocio de la organización.

Apoyo y recursos

Apoyar a las personas pertinentes y asignar recursos adecuados para el SGIA.

Mejora continua

Promover la mejora continua del SGIA y la cultura de gobernanza responsable de IA.

Evidencia de liderazgo en auditoría

En el contexto de IA, el liderazgo también implica asegurar que existan responsabilidades claras sobre los sistemas de IA, que se asignen recursos adecuados y que se tomen en cuenta riesgos e impactos relevantes en las decisiones organizacionales.

La auditoría suele buscar evidencia como:

- **Participación de la dirección en revisiones del SGIA**
- **Aprobación y comunicación de la política de IA**
- **Asignación formal de recursos**
- **Decisiones formales sobre alcance, riesgos y objetivos**
- **Seguimiento a hallazgos y acciones correctivas**

5.2

Política de IA

La organización debe establecer una política de IA apropiada al propósito de la organización y que proporcione un marco para establecer objetivos de IA. La política debe:

Apoyar los objetivos del SGIA

Orientar la consecución de los resultados previstos del sistema de gestión.

Incluir compromisos pertinentes

Cumplimiento de requisitos aplicables y compromiso con la mejora continua.

Estar disponible y comunicada

Mantenerse como información documentada, comunicarse internamente y estar disponible para partes interesadas pertinentes.

No se trata de una declaración decorativa. La política debe orientar realmente la forma en que la organización gobierna, utiliza, desarrolla o integra sistemas de IA.

Evaluación de la política en auditoría

En auditoría, la política se evalúa no solo por su existencia, sino por su **adecuación, comunicación e integración** con el sistema.
Debe ser coherente con el contexto, el alcance, los riesgos, los impactos y los objetivos definidos.
Puede buscarse evidencia como:

Elemento a verificar	Señal de alerta si...
Política aprobada y controlada	No tiene versión, fecha o aprobación formal.
Difusión interna	El personal desconoce su contenido o existencia.
Consistencia entre política y objetivos	Los objetivos no reflejan los compromisos de la política.
Referencias a principios que se reflejan en controles	Los controles no guardan relación con los compromisos declarados.

Roles, responsabilidades y autoridades

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

En un SGIA, las responsabilidades pueden abarcar:

Toma de decisiones sobre riesgos de IA	**Aprobación de controles**	**Monitoreo de impactos**	**Supervisión humana de sistemas de IA**
Gestión documental	**Evaluación del desempeño**	**Comunicación con partes interesadas**	**Tratamiento de no conformidades**

En un SGIA, no basta con afirmar que "el área de tecnología se encarga". Deben existir **responsabilidades diferenciadas y trazables**.

Evidencia de roles y responsabilidades

La evidencia puede incluir:

Descripciones de roles

Documentos que especifican funciones, responsabilidades y autoridades de cada rol dentro del SGIA.

Matrices RACI o equivalentes

Herramientas que asignan responsabilidad, autoridad, consulta e información para cada proceso o actividad del SGIA.

Organigramas funcionales

Representaciones de la estructura organizacional que muestran relaciones de autoridad y reporte.

Mandatos formales

Documentos que otorgan autoridad formal para tomar decisiones dentro del SGIA.

Registros de comunicación interna

Evidencia de que las responsabilidades han sido comunicadas y comprendidas por las personas pertinentes.

Planificación

Acciones para abordar riesgos y oportunidades

La cláusula 6 exige que la organización planifique su SGIA considerando riesgos y oportunidades, así como elementos específicos relacionados con IA. Esta planificación se desarrolla mediante cuatro apartados principales:

- **6.1.1 General**
- **6.1.2 Evaluación de riesgos de IA**
- **6.1.3 Tratamiento de riesgos de IA**
- **6.1.4 Evaluación de impacto del sistema de IA**

La función de esta cláusula es convertir el conocimiento del contexto en planificación concreta: decidir cómo se abordarán los riesgos y oportunidades del SGIA y cómo se gestionarán riesgos e impactos específicos de los sistemas de IA dentro del alcance.

General: riesgos y oportunidades del SGIA

La organización debe determinar los riesgos y oportunidades que es necesario abordar para asegurar que el SGIA pueda lograr sus resultados previstos, prevenir o reducir efectos no deseados y lograr la mejora continua.

En la práctica, esto requiere una visión amplia: no se trata solo de riesgos tecnológicos, sino también de riesgos para el sistema de gestión, para los objetivos del SGIA y para la capacidad de la organización de gobernar adecuadamente sus sistemas de IA.

La organización debe además planificar acciones para abordar estos riesgos y oportunidades, integrarlas en los procesos del SGIA y evaluar la eficacia de dichas acciones.

En auditoría, se busca evidencia de que la organización:

- **Identificó riesgos y oportunidades pertinentes**
- **Definió acciones para tratarlos**
- **Integró dichas acciones en el SGIA**
- **Evalúa si esas acciones son eficaces**

Evaluación de riesgos de IA

La organización debe establecer y mantener un proceso para evaluar riesgos de IA. Este proceso debe incluir **criterios de aceptación del riesgo** y criterios para realizar evaluaciones de riesgo de IA.
Los riesgos deben identificarse y analizarse considerando:

Los sistemas de IA dentro del alcance	**Su propósito previsto**	**El contexto de uso**	**Las partes interesadas relevantes**

Los posibles efectos sobre la organización o terceros

⚠ La evaluación de riesgos no se limita a estimar probabilidad y consecuencia de forma genérica; debe estar **conectada con el contexto real de los sistemas de IA** y con la toma de decisiones sobre controles y tratamiento.

Evidencia en evaluación de riesgos de IA

No es suficiente con tener una matriz estándar si no existen criterios claros de evaluación o si los riesgos identificados no reflejan el uso real de la IA en la organización.

El auditor puede revisar evidencia como:

Elemento de evidencia	Qué permite verificar
Metodología de evaluación de riesgos de IA	Si existe un proceso definido, documentado y aplicado.
Criterios definidos	Si la organización estableció parámetros para evaluar y aceptar riesgos.
Registros de evaluación	Si los riesgos fueron identificados, analizados y valorados con evidencia.
Vinculación entre riesgos y sistemas de IA	Si los riesgos reflejan el contexto real y conducen a decisiones de tratamiento.

Tratamiento de riesgos de IA

La organización debe establecer y mantener un proceso para tratar riesgos de IA. El tratamiento debe ser coherente con los resultados de la evaluación de riesgos y conducir a la selección de controles adecuados.

La organización debe determinar las opciones de tratamiento del riesgo de IA y comparar los controles seleccionados con los controles de referencia del **Anexo A** para verificar si se han omitido controles necesarios.

Evitar el riesgo

Decidir no realizar la actividad o uso de IA que genera el riesgo.

Mitigar mediante controles

Implementar controles que reduzcan la probabilidad o el impacto del riesgo.

Compartir el riesgo

Transferir o distribuir el riesgo con terceros, como proveedores o aseguradoras.

Aceptar el riesgo

Asumir el riesgo dentro de criterios de aceptación definidos por la organización.

Rediseñar el sistema o proceso

Modificar el sistema de IA o el proceso asociado para eliminar o reducir el riesgo en origen.

Notas sobre controles del Anexo A

Nota 1: Diseño de controles

La organización puede diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente pertinente, no exclusivamente del Anexo A.

Nota 2: Controles adicionales

Los controles enumerados en el Anexo A no son exhaustivos. Pueden incluirse controles adicionales si se necesitan para tratar riesgos específicos del contexto de la organización.

Nota 3: Aplicabilidad contextual

Debe prestarse atención al hecho de que los controles del Anexo A pueden no ser aplicables en todas las situaciones y organizaciones. La selección debe justificarse en la Declaración de Aplicabilidad (SoA).

Para el auditor, la coherencia entre la evaluación de riesgos, las opciones de tratamiento seleccionadas, los controles implementados y la Declaración de Aplicabilidad es uno de los elementos más importantes para determinar la eficacia del SGIA.

Tratamiento de riesgos de IA

El tratamiento del riesgo se refleja en la **Declaración de Aplicabilidad (SoA)**, que debe contener los controles necesarios, la justificación de inclusiones y exclusiones, y su estado de implementación.
En auditoría, este apartado es crítico porque permite conectar riesgo, control, evidencia y trazabilidad del razonamiento organizacional.

La evidencia típica incluye:

- Proceso de tratamiento del riesgo
- Criterios de selección de controles
- SoA actualizada
- Justificación de exclusiones
- Registros de implementación de controles

Evaluación de impacto del sistema de IA

La organización debe establecer y mantener un proceso para evaluar el impacto potencial que el uso previsto de los sistemas de IA puede tener sobre individuos o grupos de individuos, o sobre ambos, o sobre sociedades.

El propósito de esta evaluación es complementar la gestión de riesgos con una mirada más directa sobre consecuencias potenciales de los sistemas de IA. Puede incluir impactos sobre derechos, acceso, trato equitativo, privacidad, seguridad, autonomía, condiciones laborales, transparencia o consecuencias sociales más amplias, según el contexto.

La organización debe determinar cuándo se requiere una evaluación de impacto y cómo se documentan, revisan y utilizan sus resultados.

6.1.4 Evaluación de impacto del sistema de IA - Criterios de auditoría

Esto convierte a la evaluación de impacto en un criterio central para organizaciones cuyo uso de IA puede generar efectos significativos sobre personas o grupos.

Nota: Los detalles de una evaluación de impacto se describen en el Anexo B.

Para auditoría, no basta con confirmar que existe una plantilla de evaluación; debe revisarse si se aplica cuando corresponde, si su alcance es adecuado y si sus resultados influyen en decisiones del SGIA.

Evaluación de impacto - Evidencia

La evidencia puede incluir:

- Criterios para determinar cuándo se realiza la evaluación
- Informes de evaluación de impacto
- Registros de revisión
- Vinculación con decisiones de tratamiento del riesgo o selección de controles

Objetivos de IA y planificación para lograrlos

La organización debe establecer objetivos de IA en las funciones y niveles pertinentes. Los objetivos deben ser coherentes con la política de IA, ser medibles cuando sea posible, considerar requisitos aplicables, ser monitoreados, comunicados y actualizarse según corresponda.

Los objetivos deben ir acompañados de planificación para lograrlos, incluyendo:

- Qué se hará
- Qué recursos se requerirán
- Quién será responsable
- Cuándo se completarán las acciones
- Cómo se evaluarán los resultados

Nota: Los objetivos pueden relacionarse con desempeño del sistema, cumplimiento, supervisión humana, transparencia, calidad de datos, tratamiento de riesgos, eficacia de controles o mejora del SGIA.

Objetivos de IA - Auditoría y evidencia

No se trata de formular objetivos genéricos, sino objetivos útiles para gestionar la IA dentro del alcance del SGIA.

En auditoría, el análisis de objetivos ayuda a determinar si la organización ha traducido su política en metas concretas y si mantiene seguimiento sobre ellas.

La evidencia puede incluir:

- Objetivos documentados
- Planes asociados
- Indicadores o métricas
- Registros de seguimiento
- Acciones derivadas de desviaciones o resultados insuficientes

Planificación de cambios

Cuando la organización determina la necesidad de cambios en el SGIA, estos cambios deben realizarse de manera planificada.

Los cambios pueden estar asociados a nuevos sistemas de IA, cambios en el contexto, nuevos requisitos, hallazgos de auditoría, incidentes, cambios de proveedores, rediseño de procesos o resultados de revisión por la dirección.

En auditoría, este requisito permite revisar si los cambios son reactivos e improvisados o si existen criterios, evaluación de consecuencias, asignación de recursos y control de implementación.

Planificación de cambios - Evidencia

La evidencia puede incluir:

- Planes de cambio
- Evaluaciones previas
- Aprobaciones
- Actualización de documentación
- Seguimiento a la implementación del cambio

Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGIA. Estos recursos pueden incluir personas, infraestructura, herramientas, tecnología, tiempo, presupuesto, acceso a información, soporte especializado y mecanismos de supervisión.

Nota: Los recursos pueden ser internos o externos.

Competencia

La organización debe:

- Determinar la competencia necesaria de las personas que realizan trabajos bajo su control y que afectan el desempeño del SGIA
- Asegurar que estas personas sean competentes con base en educación, formación o experiencia apropiadas
- Conservar información documentada apropiada como evidencia de competencia

La competencia en un SGIA no se restringe al personal técnico. También puede involucrar responsables de riesgo, cumplimiento, seguridad, privacidad, áreas usuarias, dirección y auditores internos.

Nota 1: Las acciones aplicables pueden incluir la provisión de formación, mentoría o reasignación de personas actualmente empleadas; o la contratación o subcontratación de personas competentes.

Competencia - Implicaciones éticas y auditoría

> Nota 2: Una competencia adecuada puede incluir la capacidad de considerar las implicaciones éticas de las aplicaciones de IA y los riesgos conocidos y emergentes asociados a la IA, o ambas.

Para auditoría, este requisito exige revisar tanto la definición de competencias como la evidencia de que las personas pertinentes realmente las poseen.

Toma de conciencia

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

- La política de IA
- Su contribución a la eficacia del SGIA
- Los beneficios de un mejor desempeño
- Las implicaciones de no conformarse con los requisitos del SGIA

Esto implica que la organización no solo capacite, sino que logre comprensión suficiente de por qué el SGIA existe y qué consecuencias puede tener el incumplimiento.

En auditoría, suele buscarse evidencia mediante entrevistas, registros de sensibilización o materiales de comunicación interna.

Comunicación

La organización debe determinar las comunicaciones internas y externas pertinentes al SGIA, incluyendo qué comunicar, cuándo comunicar, a quién comunicar y cómo comunicar.

La comunicación en un SGIA puede referirse a políticas, responsabilidades, incidentes, riesgos, cambios, resultados de auditoría, información a usuarios, mecanismos de reclamación o interacción con autoridades y partes interesadas.

En auditoría, se revisa si la comunicación está planificada, si responde a las necesidades del SGIA y si existe evidencia de su realización.

Información documentada

El SGIA debe incluir la información documentada requerida por la norma y la información documentada que la organización determine como necesaria para la eficacia del sistema.

La información documentada puede abarcar políticas, objetivos, alcances, metodologías, evaluaciones, registros operativos, resultados de monitoreo, auditorías, revisiones y acciones correctivas.

Información documentada

El SGIA debe incluir la información documentada requerida por la norma y la información documentada que la organización determine como necesaria para la eficacia del sistema.

La información documentada puede abarcar políticas, objetivos, alcances, metodologías, evaluaciones, registros operativos, resultados de monitoreo, auditorías, revisiones y acciones correctivas.

No se trata de documentar por exceso, sino de asegurar que la organización conserva la información necesaria para planificar, operar, controlar, evaluar y mejorar el SGIA.

> Nota: La extensión de la información documentada puede diferir de una organización a otra debido al tamaño, tipo de actividades, complejidad de procesos, productos y servicios, y competencia de las personas.

En auditoría, la pregunta no es solo "¿existe un documento?", sino "¿la información documentada es suficiente, adecuada, controlada y útil como evidencia objetiva?"

Creación y actualización

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

- Identificación y descripción apropiadas
- Formato y medios adecuados
- Revisión y aprobación respecto de la idoneidad y adecuación

Esto significa que la documentación relevante del SGIA debe ser reconocible, controlada y confiable.

Para auditoría, este requisito se traduce en revisar versiones, responsables, fechas, trazabilidad de cambios y aprobación de documentos clave.

Control de la información documentada

La información documentada requerida por el SGIA y por la norma debe controlarse para asegurar que esté disponible y sea adecuada para su uso, donde y cuando se necesite, y que esté protegida adecuadamente frente a pérdida de confidencialidad, uso inadecuado o pérdida de integridad.

El control también debe abordar:

- Distribución, acceso, recuperación y uso
- Almacenamiento y preservación
- Control de cambios
- Conservación y disposición

En SGIA, esto adquiere especial relevancia cuando la documentación contiene información sensible sobre sistemas de IA, evaluaciones de impacto, tratamientos de riesgo, resultados de auditoría o decisiones de control.

Control de la información documentada - Auditoría y evidencia

Para auditoría, este apartado conecta con la confiabilidad de la evidencia. Si la información documentada no está controlada, las conclusiones del SGIA pueden perder sustento.

La evidencia puede incluir:

- Procedimientos documentales
- Sistemas de control de documentos
- Registros con control de versiones
- Matrices de acceso
- Criterios de retención y disposición

Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir requisitos y para implementar las acciones determinadas en la cláusula 6. También debe establecer criterios para los procesos y conservar información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

En SGIA, la operación traduce el sistema de gestión en práctica diaria. Aquí se verifica si lo planificado realmente se ejecuta.

Planificación y control operacional .1

Esto incluye implementar controles, operar actividades de monitoreo, aplicar criterios de aceptación, gestionar cambios planificados y revisar consecuencias de cambios no deseados, tomando acciones para mitigar efectos adversos cuando sea necesario.

Nota: La organización debe asegurarse de que los procesos externalizados se controlen o influyan.

En auditoría, este requisito es uno de los principales puentes entre documentación e implementación real.

Planificación y control operacional .2

La evidencia puede incluir:

- Procedimientos operativos
- Registros de ejecución de controles
- Criterios operacionales
- Monitoreo de procesos
- Gestión de proveedores externos
- Tratamiento de desviaciones operativas

Evaluación de impacto del sistema de IA

La organización debe realizar evaluaciones de impacto del sistema de IA en los momentos definidos por su proceso y mantener información documentada sobre los resultados.

Esta subcláusula lleva a la práctica lo establecido en 6.1.4. No basta con tener un proceso definido; deben existir evaluaciones realizadas cuando corresponda.

En auditoría, se revisa si las evaluaciones son oportunas, si cubren el alcance adecuado y si influyen en decisiones del SGIA.

Objetivos de control de IA y controles de IA

La organización debe determinar los objetivos de control de IA y los controles de IA necesarios para tratar los riesgos identificados y alcanzar niveles aceptables de riesgo. Los controles seleccionados deben compararse con el Anexo A y documentarse en la SoA.

El auditor debe revisar la lógica de selección de controles:

- Qué objetivo de control se persigue
- Qué riesgo se trata
- Qué control se seleccionó
- Si se implementó
- Cómo se evidencia su eficacia

La relación entre riesgo, objetivo de control, control y SoA es uno de los ejes más importantes del SGIA.

Controles de IA - Auditoría y evidencia

En auditoría, las incoherencias en este punto suelen producir hallazgos significativos.

La evidencia puede incluir:

- SoA
- Matrices riesgo-control
- Justificaciones de aplicabilidad
- Registros de implementación y seguimiento de controles

Implementación de los controles de IA

La organización debe implementar los controles de IA determinados en 8.3.

Esto implica que los controles no pueden quedarse en la SoA o en documentos de diseño; deben existir en la práctica y operar de acuerdo con lo planificado.

En auditoría, esta subcláusula obliga a confirmar implementación real y evidencia objetiva de funcionamiento.

MÓDULO 3

Gestión de riesgos, evaluación de impacto, tratamiento y Declaración de Aplicabilidad

Gestión de riesgos de IA

La gestión de riesgos de IA permite a la organización identificar, analizar, evaluar y priorizar los riesgos asociados con los sistemas de IA incluidos en el alcance del SGIA. Su propósito es determinar qué situaciones pueden afectar los resultados previstos del sistema de gestión o generar efectos no deseados sobre personas, procesos, servicios, productos, partes interesadas u objetivos organizacionales.

En el contexto de IA, los riesgos pueden surgir de distintas fuentes: datos insuficientes o no representativos, sesgo, falta de supervisión humana, errores en salidas de IA, uso indebido previsible, dependencia de proveedores, baja transparencia, fallas de seguridad, incumplimiento regulatorio o impactos adversos sobre individuos o grupos.

La identificación de riesgos debe ser específica. No basta con registrar expresiones generales como “riesgo de IA” o “riesgo tecnológico”. Un riesgo bien formulado debe permitir comprender qué podría ocurrir, bajo qué condiciones, qué consecuencia podría generar y qué parte del SGIA o del sistema de IA estaría involucrada.

Gestión de riesgos de IA

Para que la evaluación sea consistente, la organización debe establecer **criterios de riesgo de IA**. Estos criterios permiten diferenciar riesgos aceptables y no aceptables, comparar niveles de riesgo y tomar decisiones sobre su tratamiento. Los criterios pueden considerar:

- Probabilidad y consecuencia
- Severidad y criticidad del proceso
- Afectación a personas o grupos
- Obligaciones legales
- Capacidad de detección
- Nivel de supervisión humana
- Tolerancia al riesgo

Una vez identificados los riesgos, la organización los analiza y evalúa. El análisis permite comprender causas, consecuencias, controles existentes y nivel de exposición. La evaluación compara ese resultado con los criterios definidos para determinar si el riesgo es aceptable o si requiere tratamiento.

La priorización permite enfocar recursos y controles en los riesgos más relevantes. En sistemas de IA, esta priorización no debería basarse únicamente en criterios técnicos; también debe considerar posibles impactos sobre privacidad, seguridad, equidad, transparencia, continuidad operativa, reputación, cumplimiento y confianza de las partes interesadas.

Gestión de riesgos de IA

Después de aplicar controles o acciones de tratamiento, puede permanecer un **riesgo residual**. Este riesgo debe evaluarse frente a los criterios definidos. Si es aceptable, debe contar con aprobación según las responsabilidades establecidas por la organización. Si no es aceptable, se deben definir acciones adicionales.

La gestión de riesgos de IA requiere seguimiento. Los riesgos pueden cambiar cuando se modifican los datos, el uso previsto, el contexto de aplicación, los proveedores, los controles, la regulación o el desempeño del sistema de IA. Por esta razón, la evaluación de riesgos no debe entenderse como una actividad única, sino como un proceso que se actualiza cuando corresponde.

Evidencia relevante puede incluir: criterios de riesgo de IA, registro de riesgos, resultados de análisis y evaluación, priorización, decisiones de tratamiento, aceptación de riesgo residual y registros de seguimiento.

Evaluación de impacto del sistema de IA

La evaluación de impacto del sistema de IA permite analizar las consecuencias que pueden derivarse del desarrollo, provisión o uso de sistemas de IA. Mientras la evaluación de riesgos se enfoca en la incertidumbre y sus efectos sobre los objetivos, la evaluación de impacto se orienta a comprender cómo un sistema de IA puede afectar a individuos, grupos, organizaciones o a la sociedad.

Esta evaluación debe considerar el **uso previsto** del sistema de IA. El uso previsto define el propósito, contexto y condiciones para las cuales el sistema se diseña, proporciona o utiliza. Cuando un sistema se usa fuera de ese propósito, pueden aparecer impactos no evaluados o controles insuficientes.

También debe considerarse el uso indebido previsible, entendido como un uso no previsto, pero razonablemente anticipable. Este punto es especialmente importante en IA, porque un sistema puede utilizarse fuera de contexto, con datos inadecuados, con niveles de autonomía no previstos o para fines distintos a los definidos originalmente.

Evaluación de impacto - Niveles de análisis

La evaluación de impacto debe considerar posibles efectos en distintos niveles:

Nivel	Ejemplos de impactos
Individuos	Privacidad, acceso a servicios, trato justo, autonomía, reputación, calidad de atención
Grupos	Sesgo, discriminación, afectación diferenciada
Organizacional	Cumplimiento, confianza, continuidad operativa, seguridad, reputación, responsabilidad frente a terceros
Social	Transparencia, inclusión, derechos, seguridad pública, confianza en el uso de IA

Evaluación de impacto

Entre las dimensiones que normalmente deben analizarse se encuentran sesgo, equidad, transparencia, privacidad, seguridad, supervisión humana y rendición de cuentas. Estas dimensiones no deben tratarse como una lista aislada, sino según el contexto del sistema de IA y las partes interesadas afectadas.

La **supervisión humana** es un elemento relevante dentro de la evaluación de impacto. La organización debe considerar si existen personas con capacidad real para monitorear, revisar, intervenir o escalar situaciones cuando el sistema de IA pueda generar consecuencias relevantes. La supervisión debe ser proporcional al riesgo, al impacto y al nivel de autonomía del sistema.

La evaluación de impacto debe generar información documentada suficiente para demostrar cómo se analizaron los impactos y qué acciones se definieron. Esta información puede vincularse con la evaluación de riesgos de IA y con los controles seleccionados para tratar riesgos o reducir impactos adversos.

Tratamiento del riesgo de IA

El tratamiento del riesgo de IA consiste en seleccionar e implementar opciones para abordar los riesgos evaluados. Su propósito es modificar el riesgo hasta un nivel aceptable, de acuerdo con los criterios definidos por la organización.

Las opciones de tratamiento pueden incluir:

- Reducir el riesgo mediante controles
- Evitar una actividad
- Modificar el uso del sistema de IA
- Transferir parte del riesgo mediante acuerdos con terceros
- Aceptar el riesgo residual cuando esté justificado y aprobado

La selección de controles debe responder a los riesgos identificados. Un control no debería seleccionarse únicamente porque aparece en una lista, sino porque contribuye a tratar un riesgo, cumplir un requisito o fortalecer la eficacia del SGIA. ISO/IEC 42001 utiliza el Anexo A como referencia de controles, pero la organización puede requerir controles adicionales según su contexto, sus sistemas de IA y sus impactos.

Tratamiento del Riesgo

Cada decisión de tratamiento debe estar justificada. La organización debe poder explicar por qué selecciona un control, por qué excluye otro, qué riesgo busca tratar y cómo se verificará su implementación o eficacia. Esta justificación permite mantener trazabilidad entre riesgo, tratamiento, control y evidencia.

El tratamiento no termina con la selección de controles. Los controles deben implementarse en procesos reales, contar con responsables y conservar evidencia de ejecución. Además, la organización debe evaluar si los controles son eficaces, es decir, si producen el efecto esperado sobre el riesgo o si requieren ajustes.

Cuando el tratamiento no sea eficaz, debe revisarse. Esto puede implicar modificar controles, actualizar el plan de tratamiento, reevaluar el riesgo o establecer acciones adicionales.

El tratamiento del riesgo también debe relacionarse con los objetivos del SGIA. Si la organización ha definido objetivos relacionados con uso responsable de IA, reducción de impactos, fortalecimiento de controles, transparencia, supervisión humana o cumplimiento, los tratamientos seleccionados deberían contribuir a esos resultados.

Declaración de Aplicabilidad - SoA

La **Declaración de Aplicabilidad (SoA)** es un elemento clave del SGIA porque documenta las decisiones de control tomadas por la organización. Su función es:

- Registrar los controles necesarios
- Justificar su inclusión
- Indicar su estado de implementación
- Justificar la exclusión de controles del Anexo A cuando corresponda

La SoA no debe entenderse como una lista automática de controles. Es una declaración estructurada que conecta la evaluación de riesgos, el tratamiento seleccionado y los controles aplicables. Su valor está en demostrar que la organización revisó los controles de referencia y tomó decisiones justificadas según su contexto.

La SoA sirve para mantener trazabilidad entre riesgos, controles y decisiones de tratamiento. También permite comprender qué controles forman parte del SGIA, cuáles no aplican y por qué. Para que sea útil, debe reflejar el estado real de implementación. Si un control aparece como implementado, debe existir evidencia que respalde esa condición.

SoA - Inclusiones, exclusiones y eficacia

La revisión de la SoA debe considerar tanto inclusiones como exclusiones:

- La **inclusión** de un control debe indicar por qué es necesario, con relación al riesgo, al requisito aplicable, al objetivo del SGIA o a una decisión interna de gobierno.
- La **exclusión** de un control del Anexo A debe estar justificada de manera suficiente, considerando el alcance del SGIA, el contexto, los sistemas de IA incluidos y los riesgos evaluados.

También es importante distinguir entre implementación y eficacia. Un control puede estar definido o incluso implementado, pero eso no demuestra por sí solo que sea eficaz. La eficacia debe evaluarse mediante evidencia, resultados, seguimiento, revisiones, métricas, auditorías o registros operativos.

La SoA es uno de los documentos más importantes para la auditoría del SGIA, porque permite verificar si existe coherencia entre la evaluación de riesgos, el tratamiento, los controles, la operación y la evidencia disponible.

Anexo A - Controles de referencia

El Anexo A de ISO/IEC 42001 presenta un conjunto de controles de referencia para apoyar el tratamiento de riesgos de IA dentro del SGIA. Su función es similar a la del Anexo A en ISO/IEC 27001: no reemplaza la evaluación de riesgos ni la Declaración de Aplicabilidad, sino que proporciona una base de controles que la organización debe revisar al definir el tratamiento de riesgos.

En ISO/IEC 42001, la organización determina los controles necesarios según sus riesgos, impactos, contexto, sistemas de IA y requisitos aplicables. Posteriormente, compara esos controles con el Anexo A para verificar que no se hayan omitido controles necesarios. El resultado de esta revisión se documenta en la Declaración de Aplicabilidad (SoA).

El Anexo A no debe entenderse como una lista automática de controles obligatorios para todas las organizaciones. Su aplicación depende del alcance del SGIA, de los sistemas de IA incluidos, de los riesgos evaluados y de la justificación de aplicabilidad.

Estructura del Anexo A

El Anexo A está organizado en grupos de controles que cubren aspectos clave de la gestión de IA. Estos controles apoyan la implementación del SGIA y permiten tratar riesgos relacionados con gobierno, recursos, ciclo de vida, datos, comunicación, uso de IA y relaciones con terceros.

Grupo	Tema principal	Enfoque
A.2	Políticas relacionadas con IA	Define controles asociados con la orientación y mantenimiento de políticas de IA.
A.3	Organización interna	Aborda roles, responsabilidades, rendición de cuentas y reporte de inquietudes.
A.4	Recursos para sistemas de IA	Considera recursos, datos, herramientas, infraestructura y competencias necesarias.
A.5	Evaluación de impactos de sistemas de IA	Apoya la identificación y documentación de impactos relacionados con sistemas de IA.

Estructura del Anexo A

Grupo	Tema principal	Enfoque
A.6	Ciclo de vida del sistema de IA	Cubre objetivos, requisitos, diseño, desarrollo, verificación, validación, despliegue y documentación técnica.
A.7	Datos para sistemas de IA	Trata la gestión de datos, calidad, procedencia, preparación y uso adecuado de datos.
A.8	Información para partes interesadas	Aborda la comunicación de información relevante sobre sistemas de IA.
A.9	Uso de sistemas de IA	Considera el uso responsable, los procesos operativos y la supervisión humana.
A.10	Relaciones con terceros y clientes	Trata responsabilidades, proveedores, clientes y relaciones externas vinculadas con sistemas de IA.

Anexo B - Guía de implementación de los controles

El Anexo B de ISO/IEC 42001 proporciona orientación para implementar los controles del Anexo A. Su función es ayudar a la organización a comprender cómo aplicar los controles seleccionados, adaptándolos a su contexto, riesgos, objetivos y sistemas de IA.

A diferencia del Anexo A, que presenta controles de referencia, el Anexo B ofrece **guía de implementación**. Por tanto, no debe tratarse como una lista adicional de requisitos, sino como apoyo para aplicar controles de manera adecuada.

B.1 Generalidades

La sección B.1 explica el propósito del Anexo B. La organización puede usar esta guía para implementar controles del Anexo A, pero también puede adaptarla, ampliarla o utilizar otros enfoques si resultan más adecuados para tratar sus riesgos de IA.

El Anexo B no limita a la organización a una única forma de implementar controles.

Anexo B

B.2 Políticas relacionadas con IA

La sección B.2 orienta la implementación de controles asociados con la política de IA. Ayuda a definir cómo documentar, comunicar, revisar y alinear la política con el propósito, contexto, riesgos, valores y requisitos aplicables de la organización.

B.3 Organización interna

La sección B.3 guía la asignación de roles, responsabilidades y mecanismos internos de reporte relacionados con IA. Su propósito es fortalecer la gobernanza del SGIA y evitar vacíos de responsabilidad.

B.4 Recursos para sistemas de IA

La sección B.4 orienta la identificación y gestión de recursos necesarios para los sistemas de IA. Puede incluir recursos humanos, datos, herramientas, infraestructura, recursos computacionales y capacidades especializadas.

Anexo B

B.5 Evaluación de impactos de sistemas de IA

La sección B.5 proporciona guía para implementar controles relacionados con la evaluación de impacto del sistema de IA. Apoya la identificación, documentación y análisis de impactos sobre individuos, grupos o sociedad.

B.6 Ciclo de vida del Sistema de IA

La sección B.6 orienta controles asociados con el ciclo de vida del sistema de IA, desde el diseño y desarrollo hasta el despliegue, operación, monitoreo, mantenimiento o retiro.
Incluye aspectos como objetivos de desarrollo responsable, verificación, validación, documentación técnica, registros y criterios de operación.

B.7 Datos para sistemas de IA

La sección B.7 se enfoca en la gestión de datos utilizados por sistemas de IA. Orienta sobre adquisición, calidad, procedencia, preparación, uso y trazabilidad de datos.
Esta sección es relevante porque la calidad y gestión de los datos pueden afectar el desempeño, sesgo, fiabilidad y riesgos del sistema de IA.

Anexo B

B.8 Información para partes interesadas

La sección B.8 guía la información que debe ponerse a disposición de partes interesadas pertinentes. Puede incluir información para usuarios, documentación del sistema, condiciones de uso, limitaciones, reportes externos o comunicación de incidentes.

B.9 Uso de sistemas de IA

La sección B.9 orienta controles para el uso responsable de sistemas de IA. Ayuda a asegurar que el sistema se utilice conforme a su uso previsto, objetivos definidos, límites, instrucciones y mecanismos de supervisión.

B.10 Relaciones con terceros y clientes

La sección B.10 guía la gestión de relaciones con proveedores, terceros y clientes. Su propósito es definir responsabilidades, requisitos, información compartida, controles y expectativas cuando otras partes participan en el ciclo de vida o uso del sistema de IA.

Anexo C - Objetivos organizacionales y fuentes de riesgo

El Anexo C de ISO/IEC 42001 presenta información de apoyo sobre posibles objetivos organizacionales relacionados con IA y fuentes de riesgo asociadas. Su función es ayudar a la organización a comprender qué objetivos pueden verse influenciados por el uso, desarrollo o provisión de sistemas de IA, y qué fuentes pueden generar riesgos dentro del SGIA.

Este anexo no debe entenderse como una lista obligatoria ni exhaustiva. Su utilidad está en orientar el análisis del contexto, la evaluación de riesgos de IA, la evaluación de impacto del sistema de IA y la selección de controles.

C.1 Generalidades

La sección C.1 introduce el propósito del anexo. La organización puede utilizar esta información como referencia para identificar objetivos relevantes y fuentes de riesgo que podrían afectar el SGIA.

En la práctica, el Anexo C ayuda a ampliar la mirada de la organización más allá del desempeño técnico del sistema de IA. Permite considerar objetivos como confiabilidad, seguridad, privacidad, equidad, transparencia, rendición de cuentas, sostenibilidad, cumplimiento y generación de valor.

C.2 Objetivos organizacionales relacionados con IA

La sección C.2 presenta ejemplos de objetivos que una organización puede considerar al gestionar sistemas de IA. Estos objetivos pueden relacionarse con:

- Uso responsable de sistemas de IA
- Cumplimiento de requisitos legales, regulatorios o contractuales
- Protección de derechos y expectativas de partes interesadas
- Transparencia y comunicación adecuada
- Supervisión humana
- Seguridad y privacidad
- Calidad y confiabilidad de salidas de IA
- Equidad y reducción de sesgos
- Continuidad operativa
- Mejora del desempeño organizacional
- Confianza de clientes, usuarios y otras partes interesadas

Estos objetivos pueden servir como insumo para definir la política de IA, los objetivos del SGIA, los criterios de riesgo, la evaluación de impacto y la selección de controles.

C.3 Fuentes de riesgo relacionadas con IA

La sección C.3 presenta fuentes de riesgo que pueden considerarse en la gestión del SGIA. Estas fuentes pueden estar asociadas con:

- Datos utilizados por sistemas de IA
- Diseño, desarrollo o configuración del sistema
- Uso fuera del propósito previsto
- Uso indebido previsible
- Falta de supervisión humana
- Baja transparencia o explicabilidad
- Dependencia de proveedores
- Cambios en el contexto de aplicación
- Errores en salidas de IA
- Sesgo o resultados discriminatorios
- Vulnerabilidades de seguridad
- Incumplimiento de requisitos aplicables
- Falta de claridad en responsabilidades

Estas fuentes de riesgo ayudan a estructurar la evaluación de riesgos de IA y a determinar qué controles pueden ser necesarios.

Anexo D - Uso del SGIA en diferentes dominios o sectores

El Anexo D de ISO/IEC 42001 es informativo y explica cómo el Sistema de Gestión de Inteligencia Artificial puede aplicarse en diferentes dominios, sectores, productos y servicios.

Su propósito es mostrar que el SGIA no se implementa de la misma forma en todos los contextos. La aplicación puede variar según el sector, el tipo de sistema de IA, los requisitos aplicables, los riesgos, los impactos y las partes interesadas involucradas.

D.1 Generalidades

La sección D.1 indica que el SGIA puede utilizarse en distintos sectores, como salud, finanzas, transporte, empleo, energía, defensa u otros ámbitos donde se desarrollen, provean o usen sistemas de IA.

El anexo resalta que un sistema de IA no está compuesto únicamente por el modelo o algoritmo. También puede incluir datos, infraestructura, software, procesos, personas, interfaces y otros componentes tecnológicos. Por ello, la gestión responsable debe considerar el sistema completo.

D.2 Integración con otros sistemas de gestión

La sección D.2 explica que el SGIA puede integrarse con otros sistemas de gestión, como:

- ISO/IEC 27001 — Seguridad de la información
- ISO/IEC 27701 — Privacidad
- ISO 9001 — Calidad

Esta integración permite aprovechar estructuras existentes, evitar duplicidades y alinear la gestión de IA con otros objetivos organizacionales, como seguridad, privacidad, calidad, continuidad o cumplimiento sectorial.

MÓDULO 4

Auditorías Internas con Énfasis en Competencias de Auditor

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

Sección	Contenido
Prefacio / Introducción	Contexto y propósito de la norma
1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	Principios de auditoría
5	Administrar un programa de auditoría
6	Realización de una auditoría
7	Competencia y evaluación de los auditores

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 - Definición

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

Clasificación y definiciones fundamentales según la norma ISO 19011

A. Auditorías Internas	También 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.

Tipos de Auditoría — Detalle

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 y Evidencia de la Auditoría

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.

- 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 y Conclusiones de la Auditoría

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.

Roles en la Auditoría

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.

Roles de Apoyo en la Auditoría

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 auditoríase 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.

Conceptos Clave de la Auditoría

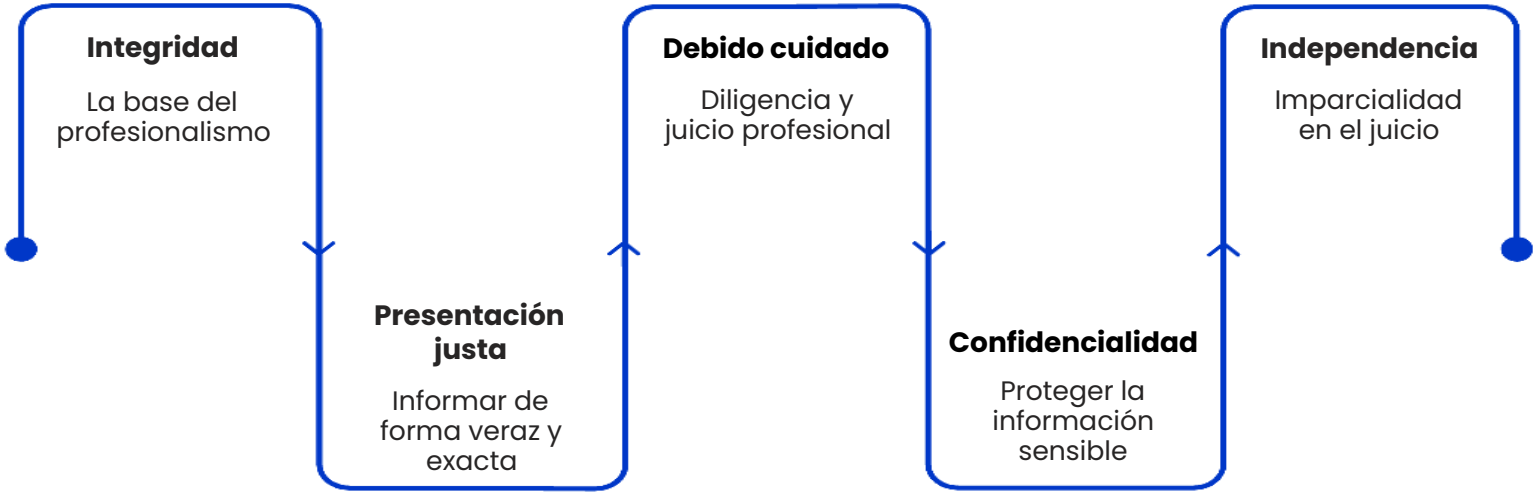
Plan de Auditoría
Descripción de las actividades y los arreglos para una auditoría.

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
- Cláusula 4: Principios de Auditoría



Métodos de Auditoría
- 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: Integridad y Presentación Justa

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.

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.

Importancia de la Tarea

El nivel de cuidado debe ser proporcional a la importancia de la tarea que se realiza.

Confianza Depositada

El auditor debe responder a la confianza del cliente de auditoría y otras partes interesadas.

Juicios Razonados

Capacidad de emitir juicios razonados en todas las situaciones 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.

Uso inapropiado	La información de auditoría no debería ser utilizada de manera inapropiada para beneficio personal por el auditor o el cliente de auditoría.
Perjuicio al auditado	No debe usarse de una manera perjudicial para los intereses legítimos del auditado.
Información sensible	Este concepto incluye el manejo adecuado de información sensible o confidencial.

Cláusula 4: Independencia

La base para la imparcialidad de la auditoría y la objetividad de las conclusiones

Independencia General

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.

Auditorías Internas

Los auditores deberían ser independientes de la función que se está auditando, si es posible. Deberían mantener la objetividad durante todo el proceso de auditoría para garantizar que los hallazgos y conclusiones se basen solo en la evidencia de auditoría.

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: Enfoque Basado en la Evidencia y en el Riesgo

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.

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 y 6: Programa y Actividades de la 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 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.

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.

Cualidades Personales

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.

Conocimientos Genéricos y Habilidades

- 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.
- 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.

Cláusula 7: Atributos Personales del Auditor

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.
h. Decisivo, es decir, capaz de llegar a conclusiones oportunas basadas en el
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) 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: Habilidades del Auditor

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.

Un auditor debería ser capaz de: .1

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.

Un auditor debería ser capaz de: .2

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:

Partes Interesadas

Necesidades y expectativas de las partes interesadas pertinentes.

Tipo de Organización

Gobernanza, tamaño, estructura, funciones y relaciones.

Gestión y Procesos

Conceptos generales de gestión y procesos empresariales relacionados.

Aspectos Culturales

Aspectos culturales y sociales del auditado.

Un auditor debería ser capaz de: .3

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	Conocimiento del lenguaje legal aplicable.
Contratación y responsabilidad	Comprensión de los marcos contractuales y de 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.

Un auditor debería ser capaz de: .4

> 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.

Alcance del programa	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.
Base del alcance	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.

Establecimiento de Objetivos del Programa de Auditoría .2

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:

a) Planificación	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	Permitir tiempo, equipo y/o capacitación insuficientes para desarrollar el programa de auditoría o realizar una auditoría.
c) Selección del equipo	Competencia global insuficiente para realizar auditorías de manera efectiva.
d) Comunicación	Procesos/canales de comunicación externos/internos ineficaces.
e) Implementación	Coordinación ineficaz de las auditorías dentro del programa de auditoría, o no considerar la seguridad y confidencialidad de la información.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría .1

f) Control de información documentada	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) Supervisión y mejora	Seguimiento ineficaz de los resultados del programa de auditoría.
h) Disponibilidad del auditado	Disponibilidad y cooperación del auditado y disponibilidad de evidencia para ser muestreada.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría .2

Las oportunidades para mejorar el programa de auditoría pueden incluir:

a) Múltiples Auditorías

Permitir múltiples auditorías en una sola visita.

b) Minimizar Desplazamientos

Minimizar el tiempo y las distancias que viajan al sitio.

c) Competencia del Equipo

Hacer coincidir el nivel de competencia del equipo de auditoría con el nivel requerido.

d) Disponibilidad del Personal

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

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 .1

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

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 Individuos que Gestionan 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.
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.

Establecer el Alcance del Programa de Auditoría .1

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.
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.
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.

Implementación del Programa de Auditoría .1

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 qué 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.

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual .2

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

En el Sitio

Las auditorías pueden realizarse presencialmente en las instalaciones del auditado.

De Forma Remota

Las auditorías pueden realizarse a distancia utilizando tecnologías de comunicación.

Combinada

El uso de estos métodos debería estar adecuadamente equilibrado, en función 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 y Determinación de Métodos de Auditoría .1

Selección del Equipo de Auditoría

A(s) persona(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.

Información para el Auditor Líder

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

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, y 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.

a) Registros del programa	• 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.
b) Registros de cada auditoría	• 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.

Administrar y Mantener los Registros del Programa de Auditoría .1

c) Registros del equipo de auditoría

- 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.

Evaluación del Programa

Las personas que gestionan el programa de auditoría deberían garantizar la evaluación de:

1. Si se están cumpliendo los cronogramas y si se están logrando los objetivos del programa de auditoría.
2. El desempeño de los miembros del equipo de auditoría, incluido el líder del equipo de auditoría y los expertos técnicos.
3. La capacidad de los equipos de auditoría para implementar el plan de auditoría.
4. Retroalimentación de clientes de auditoría, auditados, auditores, expertos técnicos y otras partes relevantes.
5. 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

Perespondido del auditor líder.

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

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.
- 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.

Planificación de Auditoría - Enfoque Basado en el Riesgo

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.

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.

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.
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).

Detalles de Planificación de Auditoría .2

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.

La planificación de la auditoría debería tener en cuenta, según corresponda:

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.

Plan de Auditoría - Contenido y Aprobación

Consideraciones de Confidencialidad y Seguimiento

- Cuestiones relacionadas con la confidencialidad y la IA.
- Cualquier acción de seguimiento de una auditoría anterior u otra(s) fuente(s), 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.

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 Talleres

Taller 1

Se recomienda por parte de la persona instructora realizar:

- Elaborar Plan de Auditoría.

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.

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.

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) Ayuda Memoria

Considerar las listas de verificación como un ayuda memoria.

b) Sin Inhibición

Evitar sentirse inhibidos por ellas.

c) Escritura Prolija

Escribir prolijamente: la lista de verificación es parte del informe de auditoría.

d) Conclusiones Finales

Registrar conclusiones finales.

e) Oportunidades de Mejora

Registrar oportunidades de mejora.

f) Identidades de Muestras

Registrar identidades específicas de las muestras examinadas.

Taller 3 y Reunión de Apertura

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.

Puntos a Considerar

Objetivos, alcance y criterios	Los objetivos, el alcance y los criterios de la auditoría.
Plan de 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	Canales de comunicación formales entre el equipo de auditoría y el auditado.
Idioma	El idioma que se utilizará durante la auditoría.
Progreso de la auditoría	El auditado debería mantenerse informado del progreso de la auditoría durante la auditoría.
Recursos e instalaciones	La disponibilidad de los recursos y las instalaciones que necesita el equipo de auditoría.
Confidencialidad e IA	Cuestiones relacionadas con la confidencialidad y la IA.
Acceso y seguridad	Acceso relevante, salud y seguridad, seguridad, emergencia y otros arreglos para el equipo de auditoría.
Actividades en el sitio	Actividades en el sitio que pueden afectar la realización de la auditoría.

Puntos a Considerar

Método de informar hallazgos

Incluye los criterios para la calificación, si corresponde.

Condiciones de terminación

Condiciones bajo las cuales puede darse por terminada la auditoría.

Tratamiento de hallazgos

Cómo tratar con posibles hallazgos durante la auditoría.

Sistema de retroalimentación

Retroalimentación del auditado sobre hallazgos o conclusiones, incluidas 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 otras actividades de auditoría y puede continuar a lo largo de la auditoría, siempre que 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.

Consulta periódica del equipo

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

Comunicación del avance

El líder del equipo auditor debe comunicar periódicamente el avance de la auditoría y cualquier inquietud al auditado.

Objetivos no alcanzables

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.

Acciones posibles

Reconfirmación o 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

Reportes de ocurrencias de eventos de seguridad, 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.

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

Las Entrevistas

Condiciones para la entrevista

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

b) Realizarse durante el horario laboral normal y, donde sea práctico, en el lugar de trabajo normal de la persona entrevistada.

c) Tratar que la persona entrevistada esté cómoda antes y durante la entrevista.

Procedimiento durante la entrevista

a) Explicar la razón para la entrevista y cualquier nota que se tome.

b) Resumir y revisar los resultados de la entrevista con la persona entrevistada.

c) Agradecer a las personas entrevistadas por su participación y cooperación.

Preguntas Claves del Auditor

Tipo de preguntas que el auditor debe formular durante la auditoría:

01

¿Realizaron auditorías internas?

02

¿Existe una política del Sistema de Gestión?

03

¿El Sistema de Gestión ha sido comunicado?

04

¿Es usted parte del grupo auditor interno?

05

¿El proceso se ejecuta como está documentado?

06

¿En dónde registra la información?

07

¿Cuál procedimiento?

08

¿Conoce la política?

09

¿Cumple la legislación?

Ejecutando la Auditoría

a) Haga un muestreo de actividades, no se centre en una.
b) Busque evidencia observando lo que ocurre y revisando registros.
c) Haga anotaciones completas.
d) Escuche las explicaciones del auditado.
e) Anote y confirme los hallazgos u observaciones. Si tiene dudas sobre el cumplimiento de un requisito podría hacer algunas preguntas abiertas adicionales.
f) 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
g) Auditoría abierta y amigable resultará en un acuerdo de que el problema existe
h) Verifique si la No Conformidad es o no puntual

Realización de Entrevistas

1

Sea amigable

Haga sentir cómodo al auditado.

2

Explique las razones

De la entrevista y de las notas tomadas.

3

Inicie con descripción

De las actividades del auditado.

4

Evite preguntas inductivas

No realizar preguntas cuya respuesta sea SÍ o NO.

5

Agradezca

Agradecer a los auditados por su participación.

Administración del Tiempo

Actividades complejas primero
Realizar primero las actividades más complejas o difíciles.

Asignar trabajo
Asignar trabajo a los otros auditores.

Inmediatez
Adquirir el hábito de hacerlo de inmediato.

Curva de cansancio
Conocer la curva de cansancio del auditado y del auditor.

Límite de tiempo
Establecer límite de tiempo y cumplirlo.

Ser creativo
Buscar soluciones innovadoras ante imprevistos.

Manejo de Situaciones Difíciles

Ausencia del responsable

A la reunión de apertura no se presenta el responsable del proceso o actividad auditada.

Falta de recursos logísticos

Se tenía previsto visitar dos instalaciones y no hay disponibles vehículos ni acompañantes.

Desvío de la pregunta

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.

Información insuficiente

El auditado suministra poca información. Ejemplo: se solicita información sobre los resultados de enero a mayo y solo presenta los resultados del último mes.

Reformulación de preguntas

El auditado reformula las preguntas del auditor.

Cuestionamiento al auditor

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

Desacuerdo en apertura

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 no evaluadas

Competencias de recurso humano no evaluada.

Controles inadecuados

Controles implementados inadecuados.

No conformidades sin cierre

No conformidades por auditorías internas sin cierre eficaz.

Acciones correctivas sin revisión

Acciones correctivas sin revisión de la dirección.

Deficiencia en análisis de riesgo

Deficiencia en metodología de análisis de riesgo.

Incumplimiento de procedimientos

Redacción de las No Conformidades

Elemento	Descripción
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	Situaciones que no representan incumplimiento, pero pueden ser revisadas por la organización para mejorar la eficacia del proceso.

Fórmula de Redacción de No Conformidades

El reporte debe contener como mínimo:

01

Visión general del hallazgo

02

Descripción completa y precisa

De lo observado.

03

Ejemplos de evidencia de auditoría

04

Referencia a la cláusula

Del estándar/documento de la organización.

05

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 hallazgos

Revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma.

Acordar conclusiones

Acordar conclusiones de auditoría.

Preparar recomendaciones

Si así lo especifica el plan de auditoría.

Las conclusiones de auditoría pueden tratar aspectos como:

Grado de cumplimiento

Evaluación del grado de cumplimiento con el criterio de auditoría.

Eficacia del sistema

Eficacia de la implementación, mantenimiento y mejoras del sistema de gestión.

Revisión por la dirección

Capacidad del proceso de revisión por la dirección para asegurar la adecuación, eficacia y mejora sostenida del SGIA.

Informe de Auditoría

El informe de auditoría debería contener:

01

Objetivos de la auditoría

02

Alcance de la auditoría

Particularmente la definición de las unidades de la organización o de los procesos auditados y el período de la auditoría.

03

Documentación de contacto

Documentación de la persona de contacto.

04

Equipo auditor

Documentación del auditor líder y otros auditores.

05

Fechas y ubicaciones

Donde se desarrollaron las actividades de la auditoría.

06

Criterio de auditoría

07

Declaraciones y conclusiones

Declaraciones de auditoría y 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:

Punto	Descripción
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:

Elemento	Descripción
a) Objetivos de auditoría	Propósito y metas de la auditoría.
b) Alcance de la auditoría	Identificación de la organización (el auditado) y las funciones o procesos auditados.
c) Cliente de auditoría	Identificación del cliente de auditoría.
d) Equipo de auditoría	Identificación del equipo de auditoría y los participantes del auditado en la auditoría.
e) Fechas y lugares	Donde se llevaron a cabo las actividades de auditoría.

Preparación y Distribución del Informe de Auditoría .1

Elemento	Descripción
f) Criterios de auditoría	Base sobre la que se evaluó la conformidad.
g) Hallazgos y evidencia	Hallazgos de auditoría y evidencia relacionada.
h) Conclusiones de auditoría	Resultados generales del proceso de auditoría.
i) Grado de cumplimiento	Una declaración sobre el grado en que se han cumplido los criterios de auditoría.
j) Opiniones divergentes	Cualquier opinión divergente no resuelta entre el equipo de auditoría y el auditado.
k) Naturaleza del muestreo	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

Plazo de emisión

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.

Fecha, revisión y aceptación

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

Distribución

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

Confidencialidad

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

Cierre y Conservación de la Información

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).

Conservación o eliminación

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.

Confidencialidad de la información

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.

Lecciones aprendidas

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:

01

Acordar la fecha

Acordar la fecha de la auditoría de seguimiento.

02

Desarrollar la auditoría

Desarrollar la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas.

03

Presentar e informar resultados

Presentar e informar los resultados de la auditoría de seguimiento.

04

Evaluar la eficacia

Evaluar la eficacia de las acciones correctivas y preventivas implantadas.

05

Informe de auditoría

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.

Confidencialidad
Protección de la información frente a accesos no autorizados.

Integridad
Garantía de exactitud y completitud de la información.

Disponibilidad
Acceso a la información cuando sea necesario.

MÓDULO 5

Evaluación del desempeño, mejora y cierre de auditoría

Intención del módulo

Este módulo desarrolla la etapa en la que el SGIA demuestra sus resultados. Después de establecer el contexto, definir responsabilidades, planificar riesgos y oportunidades, implementar controles, documentar la aplicabilidad y operar el sistema, corresponde evaluar si todo lo anterior funciona conforme a lo previsto.

Las cláusulas 9. Evaluación del desempeño y 10. Mejora permiten cerrar el ciclo del sistema de gestión. En esta etapa, la organización recopila información, analiza resultados, realiza auditorías internas, revisa el sistema desde la dirección y toma acciones para corregir desviaciones o fortalecer su desempeño.

Evaluación del Desempeño

La cláusula 9 establece los requisitos para evaluar el desempeño y la eficacia del SGIA. Esta evaluación permite determinar si el sistema está funcionando de acuerdo con lo planificado y si proporciona información suficiente para tomar decisiones, identificar desviaciones y promover la mejora.

La evaluación del desempeño se apoya en los elementos previamente definidos por la organización: objetivos de IA, riesgos, controles, procesos operativos, información documentada, resultados de seguimiento, auditorías internas y revisión por la dirección.

La cláusula 9 se compone de tres apartados:

9.1

Seguimiento, medición, análisis y evaluación.

9.2

Auditoría interna.

9.3

Revisión por la dirección.

En conjunto, estos apartados permiten verificar si el SGIA se mide, se audita y se revisa de manera planificada. También proporcionan información para determinar si el sistema requiere ajustes, acciones correctivas o mejoras.

Mejora Continua

La subcláusula 10.1 establece que la organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGIA.

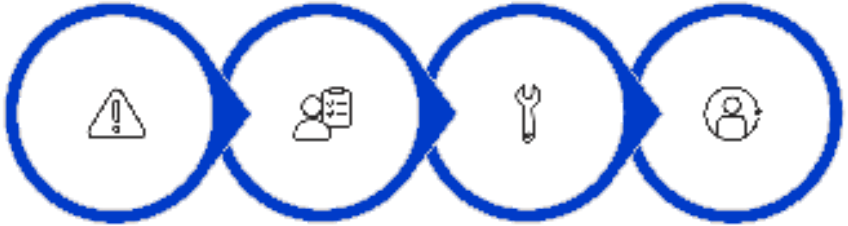
La mejora continua puede apoyarse en resultados de seguimiento y medición, auditorías internas, revisión por la dirección, cambios en el contexto, desempeño de controles, resultados de evaluaciones de riesgos de IA o evaluaciones de impacto del sistema de IA.

En el SGIA, la mejora puede reflejarse en actualización de procesos, ajustes a controles, cambios en objetivos, revisión de la SoA, fortalecimiento de competencias o actualización de información documentada.

No Conformidad y Acción Correctiva

La subcláusula 10.2 establece que, cuando ocurre una no conformidad, la organización debe reaccionar ante ella, controlarla, corregirla y abordar sus consecuencias.

También debe evaluar la necesidad de acción correctiva para eliminar la causa de la no conformidad y evitar que vuelva a ocurrir o que ocurra en otra parte del SGIA. La organización debe conservar información documentada sobre la naturaleza de la no conformidad, las acciones tomadas y los resultados de dichas acciones.



No Conformidad y Acción Correctiva .2

Ejemplos de información documentada que debe conservarse:

1. **Registro de no conformidad**
2. **Análisis de causa**
3. **Plan de acción correctiva**
4. **Evidencia de implementación**
5. **Verificación de eficacia**

Integración Final del SGIA

La integración final del SGIA permite comprender cómo los elementos desarrollados en la norma se conectan entre sí para formar un sistema de gestión completo. El SGIA no debe operar como un conjunto de actividades aisladas, sino como una estructura integrada que relaciona contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora.

El contexto permite identificar las condiciones internas y externas, las partes interesadas y el alcance del SGIA. El liderazgo proporciona dirección, política, responsabilidades y recursos. La planificación define riesgos, oportunidades, objetivos, tratamientos y cambios. El soporte asegura recursos, competencia, comunicación e información documentada. La operación implementa procesos, controles, evaluaciones de riesgos y evaluaciones de impacto. La evaluación del desempeño permite medir, auditar y revisar el sistema. Finalmente, la mejora permite corregir desviaciones y fortalecer la eficacia del SGIA.

Esta integración también se observa en la relación entre riesgos, controles y evidencia. Los riesgos de IA identificados deben conducir a tratamientos adecuados; los tratamientos deben reflejarse en controles; los controles aplicables deben justificarse en la Declaración de Aplicabilidad; y la implementación debe demostrarse mediante información documentada.

Integración final del SGIA .1

Esta integración también se observa en la relación entre riesgos, controles y evidencia.

Elemento del SGIA	Función dentro del sistema
Contexto y alcance	Define la realidad organizacional y los límites del SGIA.
Liderazgo y política de IA	Establece dirección, compromiso y responsabilidades.
Riesgos, impactos y objetivos	Orientan la planificación y priorización del sistema.
Controles y SoA	Documentan decisiones de tratamiento y aplicabilidad.
Soporte y operación	Permiten implementar y mantener el SGIA.
Evaluación del desempeño	Verifica resultados, conformidad y eficacia.
Mejora	Corrige desviaciones y mantiene la evolución del sistema.

La idea central es que cada cláusula cumple una función dentro del ciclo de gestión. Ningún requisito debe verse de forma aislada. La eficacia del SGIA depende de la coherencia entre lo que la organización define, implementa, mide, revisa y mejora.

Integración final del SGIA .2

La integración final también ayuda a comprender el cierre de auditoría. Un hallazgo puede originarse en una falla documental, operativa o de control, pero normalmente se relaciona con más de una parte del sistema. Por ejemplo, una debilidad en la implementación de controles puede estar conectada con una evaluación de riesgos incompleta, una SoA desactualizada, falta de competencia o seguimiento insuficiente.

Por ello, al revisar un SGIA, es importante mantener una visión de sistema. La conformidad no se demuestra únicamente por la existencia de documentos, sino por la coherencia entre requisitos, decisiones, controles, evidencias y resultados.

¿Quién es Certiprof®?

Certiprof® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **ATPs (Authorized TrIAning Partners.)**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos cionales.

Nuestras Afiliaciones

Aprendizaje Permanente

- Certiprof ha creado una insignia especial para reconocer a los aprendices constantes.
- Para el 2024, se han emitido más de 1,000,000 de estas insignias en más de 11 idiomas.

Propósito y Filosofía

- Esta insignia está destinada a personas que creen firmemente en que la educación puede cambiar vidas y transformar el mundo.
- La filosofía detrás de la insignia es promover el compromiso con el aprendizaje continuo a lo largo de la vida.

Acceso y Obtención de la Insignia

- La insignia de Lifelong Learning se entrega sin costo a aquellos que se identifican con este enfoque de aprendizaje.
- Cualquier persona que se considere un aprendiz constante puede reclamar su insignia visitando:

COMPARTE Y VERIFICA

TUS LOGROS DE APRENDIZAJE

FÁCILMENTE

#I42001LA #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com