# AI GOVERNANCE

PROFESSIONAL CERTIFICATION


certiprof®

AIGPC™ VERSIÓN 042026

# ISO/IEC 42001: Material de Autoestudio y de Apoyo para los Programas de Certificación AIMPC™ y AIGPC™

## Módulo 1. Fundamentos del Sistema de Gestión de Inteligencia Artificial

### Introducción al módulo

La primera parte del documento cumple una función niveladora. Antes de entrar en responsabilidades, controles o evaluación del desempeño, el participante necesita construir una base conceptual sólida sobre la naturaleza del SGIA, el origen de la norma y la lógica sistémica que la recorre.

La inteligencia artificial se consolida como una de las capacidades tecnológicas con mayor influencia sobre la productividad, la innovación y la transformación de modelos de negocio. Su adopción ya no se concentra en laboratorios avanzados ni en compañías nativas digitales. Se extiende a procesos de atención al cliente, análisis de datos, automatización documental, detección de patrones, soporte a decisiones, control operacional, personalización de servicios y numerosas funciones transversales. Ese crecimiento, sin embargo, no produce únicamente beneficios. También introduce incertidumbres nuevas: opacidad de resultados, sesgos, degradación del desempeño, dependencia de terceros, dificultad de supervisión, impacto sobre personas, tensiones regulatorias y exigencias crecientes de rendición de cuentas.

En este contexto, ISO/IEC 42001 aparece como un marco de dirección y control específicamente orientado a la IA. No se limita a describir buenas prácticas técnicas. Tampoco se restringe a la lógica de un checklist de cumplimiento. En realidad, propone algo más ambicioso: tratar la IA como una capacidad organizacional que debe ser gobernada mediante política, objetivos, procesos, recursos, controles, evaluación del desempeño y mejora continua. Ese es el punto de partida de un Sistema de Gestión de Inteligencia Artificial, o SGIA.

Para un programa de certificación, esta idea resulta decisiva. El participante no solo necesita identificar cláusulas o recordar terminología. Necesita entender que la IA cambia la manera en que la organización asume riesgos, distribuye responsabilidades, documenta decisiones y protege su legitimidad frente a clientes, reguladores, usuarios y órganos de gobierno. Por esa razón, el estudio de ISO/IEC 42001 comienza con fundamentos. Antes de entrar en contexto, liderazgo, planificación u operación, es necesario comprender por qué la norma existe, qué resuelve y qué tipo de disciplina de gestión busca instalar dentro de la organización.

## 1. Introducción

La creciente adopción de la inteligencia artificial exige pasar de un enfoque meramente tecnológico a un enfoque de gestión. Mientras la IA se usa para ampliar capacidades, acelerar tareas o mejorar resultados, las organizaciones también enfrentan una pregunta más exigente: cómo asegurar que ese uso sea responsable, trazable, alineado con sus objetivos y defendible frente a terceros. Este primer bloque del material de autoestudio fija con claridad esa tensión entre oportunidad y responsabilidad.

La IA puede generar ventajas competitivas reales. Puede reducir tiempos de procesamiento, mejorar la capacidad de análisis, ampliar el alcance del servicio y fortalecer la toma de decisiones. Ahora bien, también puede producir consecuencias no deseadas cuando se incorpora sin criterios de gobierno. Un sistema puede ofrecer resultados eficaces desde el punto de vista técnico y, aun así, ser inadecuado desde una perspectiva ética, regulatoria, reputacional o social. Puede ser útil para el área que lo impulsa y al mismo tiempo crear incertidumbre para la organización en su conjunto.

Por eso, la apertura de este módulo no debe quedarse en una descripción general de la IA. Debe dejar establecido que la gestión responsable de la inteligencia artificial requiere estructuras de decisión más robustas que las normalmente utilizadas para otras herramientas digitales. La razón es sencilla: la IA puede modificar procesos, influir en personas, alterar criterios de selección, priorizar información, automatizar juicios parciales y producir efectos difíciles de explicar o anticipar. Eso exige una forma de gobierno que conecte estrategia, operación y supervisión.

ISO/IEC 42001 se presenta, precisamente, como esa base. Permite a la organización estructurar su relación con la IA mediante un sistema capaz de sostener consistencia, trazabilidad y mejora. En lugar de reaccionar caso por caso, la organización construye un marco estable para definir qué hace con la IA, por qué lo hace, bajo qué criterios la controla y cómo corrige desviaciones. Desde la lógica de AIMPC™ y AIGPC™, esta introducción debe leerse como una invitación a pensar la IA no solo como innovación, sino como responsabilidad institucional.

## 2. Sistema de Gestión de Inteligencia Artificial (SGIA)

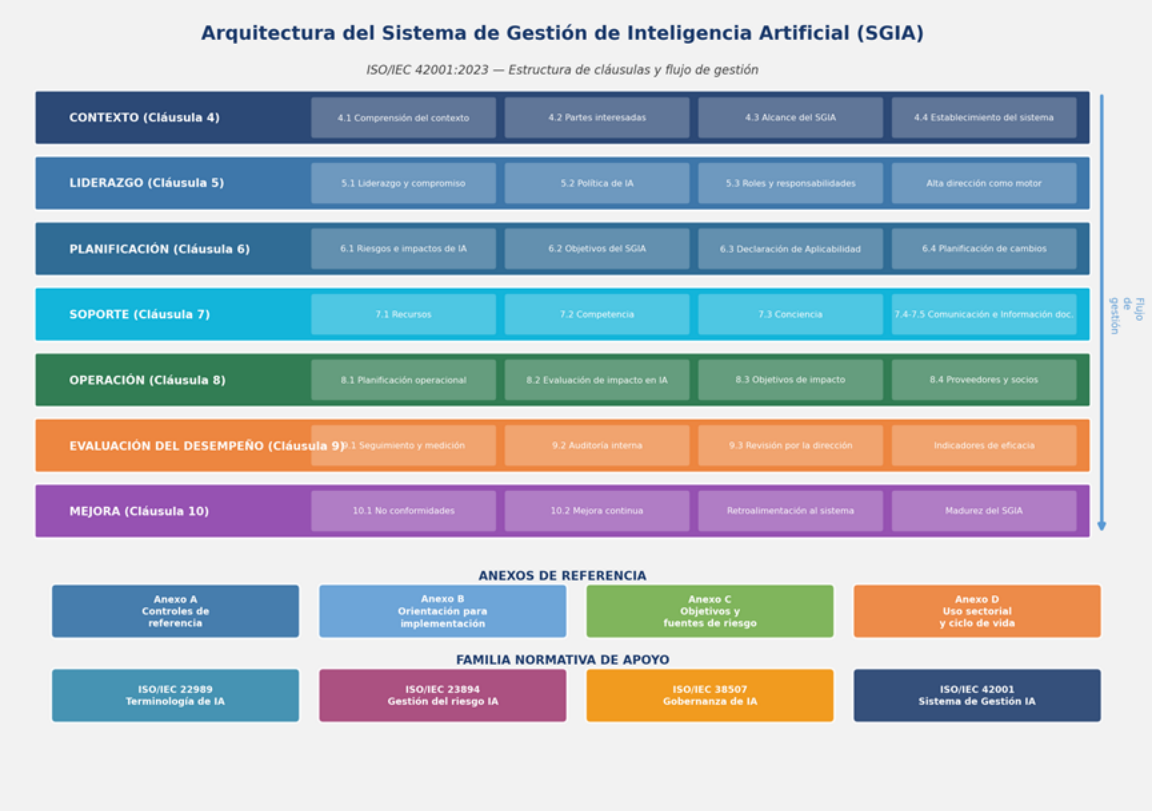
ISO/IEC 42001 establece requisitos para diseñar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Inteligencia Artificial. Esta afirmación parece simple, pero contiene una transformación profunda. Significa que la IA deja de administrarse como una suma de iniciativas dispersas y pasa a tratarse como una capacidad que exige dirección, coordinación, control y evaluación permanente.

Un SGIA no es un software. No es un comité aislado. No es una política colgada en la intranet. Es el conjunto de elementos interrelacionados que permiten a la organización orientar sus decisiones sobre IA con disciplina de gestión. Eso incluye liderazgo visible, definición de políticas, asignación de responsabilidades, establecimiento de objetivos, identificación de riesgos, diseño de controles, provisión de recursos, conservación de información documentada, seguimiento del desempeño y mejora continua. Dicho de otro modo, el SGIA funciona como la arquitectura que convierte la intención organizacional en práctica consistente.

La norma enfatiza que la aplicación de sus requisitos debe centrarse en las características propias de la IA. Ese matiz es importante. No todas las tecnologías plantean los mismos desafíos. En IA aparecen rasgos particulares que exigen salvaguardas específicas: aprendizaje continuo, dificultad de explicación, dependencia de datos, variabilidad del desempeño, opacidad de ciertos modelos, autonomía parcial en la generación de resultados, cambios por interacción con el entorno y sensibilidad especial a contextos de uso. Por ello, un SGIA no replica sin más la lógica de otros sistemas. La adapta al hecho de que la IA introduce incertidumbres particulares.

Desde el punto de vista operativo, el SGIA permite ordenar procesos y responsabilidades. Ayuda a identificar quién diseña, quién aprueba, quién supervisa, quién documenta, quién comunica y quién corrige. Desde el punto de vista estratégico, su valor es aún mayor: instala un marco de gobierno que permite a la alta dirección comprender la exposición real que la IA genera, alinear decisiones con la estrategia institucional y sostener una postura responsable frente a partes interesadas.

Conviene insistir aquí en una idea central para el autoestudio: el SGIA no busca frenar la innovación. Busca hacerla sostenible. Una organización madura no renuncia a la IA por la existencia de riesgos. La gestiona mejor. Identifica dónde la IA aporta valor, qué límites requiere, qué evidencias debe conservar y qué supervisión es necesaria para que esa aportación no se convierta en una fuente de vulnerabilidad. Ese equilibrio entre habilitar y controlar es, precisamente, uno de los núcleos conceptuales de ISO/IEC 42001.




## 3. Historia de la norma

La norma fue preparada por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnologías de la Información, Subcomité SC 42, Inteligencia Artificial. Este origen merece más atención de la que suele recibir en materiales resumidos. No es un simple dato institucional. Indica que ISO/IEC 42001 forma parte de un esfuerzo formal y coordinado de normalización internacional en torno a la IA.

Ese proceso de elaboración refuerza la legitimidad de la norma por varias razones. En primer lugar, porque surge dentro del ecosistema habitual de producción normativa de ISO e IEC, donde los organismos nacionales participan a través de comités técnicos especializados. En segundo lugar, porque su construcción no responde a una sola visión local, sectorial o empresarial, sino a un diálogo técnico internacional orientado a generar un referente aplicable en múltiples contextos. En tercer lugar, porque se integra en un campo de trabajo más amplio sobre IA, lo que permite que sus requisitos dialoguen con normas complementarias de conceptos, riesgo y gobernanza.

Para el participante, esta historia debe traducirse en una conclusión práctica: ISO/IEC 42001 no es una guía improvisada ni una moda pasajera. Es un referente construido dentro del sistema internacional de normalización técnica. Esa base institucional fortalece su valor comercial, su autoridad como marco de certificación y su utilidad para

organizaciones que necesitan mostrar a terceros que gestionan la IA de acuerdo con una estructura reconocida.

Además, comprender el origen de la norma ayuda a interpretar correctamente su tono. ISO/IEC 42001 no adopta el lenguaje de una política pública ni el de un marco filosófico. Habla como norma de sistema de gestión. Eso significa que organiza responsabilidades, define requisitos, orienta procesos y exige evidencia. Quien la estudia debe leerla como una herramienta de conducción institucional, no como una reflexión abstracta sobre tecnología.

## 4. Estructura de ISO/IEC 42001:2023

La estructura de ISO/IEC 42001 sigue una secuencia que responde a la lógica de un sistema de gestión integral. Comienza con alcance, referencias normativas y términos, y luego avanza hacia contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Vista en superficie, esta secuencia puede parecer una división convencional de capítulos. En realidad, expresa un recorrido de gestión muy preciso.

Primero, la organización comprende dónde está y qué factores condicionan su SGIA. Después, la alta dirección establece orientación y compromiso. Luego, la organización traduce esa orientación en riesgos, impactos, objetivos y planes. Más tarde habilita recursos, competencias, comunicación e información documentada. A continuación ejecuta controles y procesos. Finalmente, evalúa resultados y corrige o mejora el sistema. La norma no se limita a enumerar asuntos. Describe el movimiento completo de un sistema que piensa, actúa, mide y aprende.

Esta estructura tiene implicaciones relevantes para la formación. El candidato no debe memorizar cláusulas como compartimentos aislados. Debe entender su encadenamiento. Una evaluación de riesgos sin claridad de contexto será débil. Una política de IA sin liderazgo efectivo será decorativa. Un control operacional sin recursos adecuados será inestable. Una revisión por la dirección sin indicadores confiables será superficial. La fortaleza del SGIA depende, precisamente, de la interacción entre sus partes.

Otro aspecto relevante es la alineación con la estructura armonizada utilizada por las normas modernas de sistemas de gestión. Esa armonización favorece la integración del SGIA con capacidades organizacionales ya existentes, como calidad, seguridad de la información, privacidad, cumplimiento o continuidad. Desde un enfoque senior, esto resulta especialmente valioso: la IA no necesita gobernarse como una isla. Puede integrarse con estructuras previas, siempre que se respeten sus riesgos y particularidades.

## 5. Ciclo Deming PHVA y SGIA

ISO/IEC 42001 se comprende mejor cuando se interpreta desde el ciclo PHVA: planificar, hacer, verificar y actuar. Esta lógica, ampliamente utilizada en sistemas de gestión, permite entender el SGIA como un mecanismo dinámico y no como una estructura estática.

Planificar implica comprender el contexto, identificar partes interesadas, establecer objetivos, definir criterios de riesgo, anticipar impactos y decidir qué controles serán necesarios. Hacer implica ejecutar procesos, asignar recursos, operar controles, formar personas y desplegar el sistema en condiciones reales. Verificar exige monitorear, medir, revisar, analizar y obtener información útil sobre la eficacia del SGIA. Actuar supone corregir, ajustar, fortalecer y mejorar continuamente el sistema a partir de los hallazgos obtenidos.

Lo verdaderamente decisivo es que este ciclo evita dos errores frecuentes. El primero es pensar la gestión de IA como un esfuerzo puntual, limitado al momento del despliegue. El segundo es creer que basta con controlar técnicamente el sistema sin revisar sus efectos, su contexto o la vigencia de sus decisiones. El PHVA recuerda que la gestión responsable de IA nunca termina del todo. Se reevalúa, se recalibra y se fortalece con el tiempo.

En clave comercial y de certificación, el PHVA también aporta una narrativa poderosa. Permite mostrar que la organización no improvisa. Planifica antes de actuar, mide antes de decidir y mejora antes de repetir errores. Ese comportamiento organizacional proyecta madurez. Y la madurez, en el terreno de la IA, se traduce en confianza.

## 6. ISO/IEC 42001 y la familia de normas de apoyo

Dentro del ecosistema normativo asociado a ISO/IEC 42001, algunas referencias cumplen una función decisiva. ISO/IEC 22989:2022 proporciona conceptos y terminología. ISO/IEC 23894:2023 ofrece orientación específica sobre gestión del riesgo de IA. ISO/IEC 38507:2022 vincula la gobernanza de IA con las responsabilidades del órgano de dirección. Cada una aporta una pieza distinta, y juntas refuerzan la capacidad de la organización para interpretar e implementar el SGIA con mayor solidez.

ISO/IEC 22989 resulta esencial porque evita ambigüedad semántica. En sistemas de gestión, el lenguaje importa. Cuando distintas áreas usan los mismos términos con significados diferentes, la implementación pierde coherencia. Por eso, una base terminológica común no es una formalidad académica. Es un requisito práctico para la eficacia del sistema.

ISO/IEC 23894 amplía la comprensión del riesgo en entornos de IA. Ayuda a traducir incertidumbres técnicas, organizacionales y sociales en criterios de evaluación y tratamiento. Su valor es alto porque recuerda que el riesgo de IA no se limita al fallo técnico. También involucra consecuencias sobre individuos, grupos, reputación, cumplimiento y legitimidad.

ISO/IEC 38507, por su parte, aporta una mirada de gobernanza especialmente útil para AIGPC™. Sitúa la IA en el nivel de dirección y supervisión, no solo en el nivel de ejecución. Esto permite al profesional conectar la implementación de controles con las responsabilidades más amplias del liderazgo institucional.

## Cierre del módulo 1

Al cierre de este primer módulo, el participante debe haber consolidado varias ideas clave. La primera es que la IA necesita gobierno, no solo capacidad técnica. La segunda es que ISO/IEC 42001 ofrece una estructura formal para ese gobierno, organizada como sistema de gestión. La tercera es que el SGIA conecta procesos, controles, riesgo, liderazgo y mejora continua en una sola arquitectura. La cuarta es que la norma se apoya en una familia de referencias complementarias que fortalecen terminología, gestión del riesgo y gobernanza.

En la progresión del documento, este módulo establece el lenguaje de entrada. El siguiente módulo estrecha el foco: pasa de los fundamentos generales a las definiciones y límites que permiten interpretar la norma con precisión operativa.

En síntesis, este módulo no es una antesala decorativa. Es el fundamento conceptual sobre el cual se sostiene toda la construcción posterior. Sin esta base, las cláusulas siguientes pueden leerse como requisitos dispersos. Con ella, en cambio, se entienden como partes de una misma decisión estratégica: gestionar la IA de manera responsable, consistente y defendible.

# Módulo 2. Alcance, referencias normativas y términos

## Introducción al módulo

Si el módulo anterior explicó por qué la IA necesita un sistema de gestión, este segundo módulo define el perímetro conceptual y normativo con el que debe interpretarse ese sistema. Su función dentro de la estructura global es convertir una comprensión general en una comprensión técnicamente precisa.

Todo sistema de gestión necesita un lenguaje preciso y un perímetro claro. Antes de determinar responsabilidades, riesgos o controles, la organización debe saber qué cubre la norma, qué referencias son indispensables para interpretarla y qué significado técnico tienen los términos con los que se construirá el sistema. Por eso, este módulo ocupa una posición fundamental dentro del autoestudio. No se trata de una sección preliminar de baja relevancia. Se trata del vocabulario operativo y conceptual del SGIA.

Cuando una organización interpreta mal el alcance, sobredimensiona o subestima su responsabilidad. Cuando usa referencias normativas de forma superficial, debilita la coherencia de su implementación. Cuando no comparte definiciones estables, cada área termina entendiendo una cosa distinta por riesgo, política, desempeño, competencia o parte interesada. En consecuencia, el sistema pierde unidad. Dicho de otro modo, los términos importan porque ordenan la realidad de la organización.

Este módulo, por tanto, debe estudiarse con atención. Aquí se define quién puede aplicar la norma, qué documentos son necesarios para su interpretación y cómo deben entenderse conceptos básicos para que la gestión de la IA no dependa de intuiciones dispersas. También se establece la transición desde una lectura general del SGIA hacia una comprensión más fina de los elementos que lo componen.

## 7. Cláusula 1: Alcance

ISO/IEC 42001 especifica requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de inteligencia artificial dentro del contexto de una organización. Está dirigida a organizaciones que proporcionan o utilizan productos o servicios que emplean sistemas de IA. Esta formulación debe leerse con cuidado porque define una aplicabilidad amplia.

La norma no se restringe a empresas que desarrollan modelos de IA desde cero. También abarca organizaciones que integran soluciones de terceros, utilizan IA para procesos internos, ofrecen servicios apoyados por IA o incorporan sistemas inteligentes dentro de productos más amplios. Esta amplitud es esencial para el profesional de certificación, ya

que desmonta una idea equivocada muy común: creer que ISO/IEC 42001 solo es relevante para compañías tecnológicas especializadas.

En la práctica, una organización puede necesitar un SGIA aunque su negocio principal no sea la tecnología. Basta con que la IA influya de manera significativa sobre decisiones, operaciones, servicios, relaciones con clientes, tratamiento de datos o exposición al riesgo. Un hospital que utiliza sistemas de apoyo diagnóstico, una entidad financiera que automatiza priorización de casos, una universidad que integra herramientas de análisis predictivo, una empresa logística que usa modelos para planificación o una administración pública que incorpora IA en atención ciudadana pueden requerir un sistema de gestión de IA plenamente estructurado.

Desde una perspectiva de implementación, la cláusula de alcance obliga a una pregunta estratégica: en qué medida la IA forma parte del valor que la organización produce o del riesgo que debe gestionar. Y desde la gobernanza, obliga a otra pregunta igual de importante: hasta dónde llega la responsabilidad institucional por los efectos del uso, desarrollo o provisión de esa IA. La respuesta a ambas preguntas condiciona todo el diseño posterior del SGIA.

## 8. Cláusula 2: Referencias normativas

La cláusula de referencias normativas define qué documentos resultan necesarios para la correcta aplicación de ISO/IEC 42001. En este caso, la referencia central es ISO/IEC 22989:2022, enfocada en conceptos y terminología de inteligencia artificial. Aunque esta cláusula suele parecer breve, su impacto práctico es considerable.

Toda norma de sistema de gestión depende de una interpretación consistente de sus conceptos. Si la organización no comparte significados estables, los procesos se fragmentan. Un área puede entender una cosa por sistema de IA, otra por uso previsto y otra por parte interesada. Esa dispersión complica la evaluación del riesgo, debilita la documentación y dificulta la rendición de cuentas. ISO/IEC 22989 funciona, precisamente, como el lenguaje base que permite alinear esas interpretaciones.

En clave aplicada, esta referencia cumple tres funciones. Primero, aporta precisión conceptual. Segundo, mejora la coordinación entre perfiles técnicos, jurídicos, de cumplimiento y de negocio. Tercero, reduce la probabilidad de que el SGIA se construya sobre términos difusos o contradictorios. Lo que parece una simple referencia documental es, en realidad, una condición para la coherencia operativa del sistema.

En un entorno de autoestudio, este punto merece especial atención. El candidato debe comprender que una referencia normativa no se cita por erudición. Se utiliza porque la norma la necesita para desplegar su propio significado. Sin ese apoyo terminológico, la implementación queda expuesta a interpretaciones débiles o inconsistentes.

## 9. Cláusula 3: Términos y definiciones

La cláusula 3 establece que, para los propósitos de ISO/IEC 42001, aplican los términos y definiciones de ISO/IEC 22989 junto con los adicionales incluidos en la propia norma. Este bloque no debe tratarse como un glosario accesorio. En los sistemas de gestión, las definiciones no solo describen. Delimitan. Establecen cómo la organización entiende su realidad y cómo convierte requisitos abstractos en decisiones concretas.

Un SGIA eficaz necesita que los conceptos esenciales sean interpretados de manera consistente por la alta dirección, los responsables de proceso, las funciones de control, los equipos técnicos y cualquier otra parte involucrada. Cuando eso ocurre, la política se redacta con mayor claridad, los objetivos se formulan con más precisión, la documentación gana coherencia y el sistema se vuelve más defendible frente a revisiones internas, auditorías o procesos de certificación.

A continuación, se desarrollan las definiciones más relevantes como unidades pedagógicas del módulo.

## 10. Organización (3.1)

La norma define organización como una persona o grupo de personas que tiene funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. Esta definición parece amplia, y precisamente por ello es útil. Incluye empresas, asociaciones, instituciones, autoridades, organizaciones benéficas y otras formas organizativas, públicas o privadas.

En el contexto del SGIA, esta definición cumple una función esencial: delimitar quién asume responsabilidad por el sistema. Cuando la organización forma parte de una entidad mayor, el término se refiere solo a la parte incluida dentro del alcance del SGIA. Esta precisión es especialmente relevante en grupos empresariales, estructuras multinacionales, corporaciones descentralizadas o implementaciones parciales por unidad de negocio.

En términos operativos, definir correctamente la organización ayuda a ubicar funciones, dependencias, relaciones internas y límites de control. En clave estratégica, fija el perímetro dentro del cual la dirección responderá por el sistema de gestión de IA. En otras palabras, la definición de organización no es genérica. Es una decisión estructural del sistema.

## 11. Parte interesada (3.2)

La norma considera parte interesada a toda persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o actividad. En un SGIA, esta definición tiene un peso especial porque la IA puede producir efectos dentro y fuera de la organización.

Las partes interesadas no se limitan a clientes o reguladores. También pueden incluir usuarios, empleados, proveedores, socios, comunidades impactadas, órganos de dirección, entes de supervisión, titulares de datos, equipos internos de soporte, áreas jurídicas o cualquier actor cuya relación con la IA sea relevante para el sistema. El valor de esta definición está en ampliar la mirada. La organización no gestiona IA únicamente para sí misma. La gestiona dentro de un ecosistema de expectativas, obligaciones y posibles impactos.

En términos de implementación, reconocer partes interesadas permite identificar requisitos relevantes, organizar mecanismos de comunicación, priorizar controles y comprender mejor el efecto potencial de las decisiones vinculadas con IA. En clave de gobernanza, fortalece legitimidad y anticipa presión reputacional o regulatoria.

## 12. Alta dirección (3.3)

La alta dirección es la persona o grupo de personas que dirige y controla la organización al más alto nivel. Esta definición resulta crítica porque evita relegar la IA a un terreno puramente técnico. ISO/IEC 42001 sitúa la responsabilidad última del sistema en el nivel directivo.

La norma aclara que la alta dirección puede delegar autoridad y proporcionar recursos. Sin embargo, delegar no equivale a desentenderse. El liderazgo del SGIA exige patrocinio, orientación estratégica y capacidad de priorización. Cuando la alta dirección se involucra activamente, el sistema gana legitimidad, recursos y capacidad de integración con los procesos de negocio.

Para el participante, esta definición debe convertirse en una idea nítida: la IA no se gobierna únicamente desde tecnología. Requiere compromiso ejecutivo. Y ese compromiso no se demuestra con discursos, sino con política, objetivos, recursos, seguimiento y decisiones de mejora.

## 13. Sistema de gestión (3.4)

La norma define sistema de gestión como el conjunto de elementos interrelacionados o que interactúan dentro de una organización para establecer políticas y objetivos, así como procesos para lograr esos objetivos. Esta definición es central. Ayuda a entender que un SGIA no es un documento, un área, una herramienta ni una auditoría periódica. Es una estructura integrada.

En términos de implementación, esto implica diseñar relaciones entre política, procesos, métricas, responsabilidades, controles y mejora. El valor del sistema radica, precisamente, en cómo conecta decisiones aparentemente distintas para producir una respuesta organizacional coherente frente a la IA. En clave de gobernanza, permite pasar de iniciativas aisladas a un esquema estable de dirección y control.

## 14. Política (3.5)

La política es la expresión formal de las intenciones y la dirección de la organización. En un SGIA, la política de IA fija el marco desde el cual la organización declara cómo entiende, orienta y limita su relación con la IA.

Una política bien formulada no sirve solo para cumplir con la norma. Sirve para alinear liderazgo, riesgo, prioridades, controles y comportamiento esperado. Establece el tono institucional. Define qué principios guían la adopción o el uso de la IA. Y facilita que las decisiones posteriores mantengan coherencia. Por eso, en el estudio de esta definición, conviene leer la política como punto de partida de la gobernanza, no como pieza documental aislada.

## 15. Objetivo (3.6)

La norma define objetivo como el resultado a lograr y aclara que puede ser estratégico, táctico u operativo. Esta definición es breve, pero muy poderosa. Los objetivos convierten una intención general en dirección concreta.

Dentro del SGIA, los objetivos permiten priorizar recursos, asignar responsabilidades, definir métricas y revisar resultados. Sin objetivos claros, el sistema pierde dirección. Con objetivos bien construidos, la organización puede transformar su política de IA en compromisos verificables. En clave de gestión, esto es esencial. En clave de gobernanza, también, porque ayuda a mostrar que la IA se administra por resultados y no por intuición.

## 16. Riesgo (3.7)

El riesgo se define como el efecto de la incertidumbre sobre los objetivos. La norma recuerda que ese efecto puede ser positivo o negativo. Esta definición debe estudiarse con amplitud, porque en IA la incertidumbre adopta formas especialmente variadas.

Riesgo no es solo fallo técnico. También puede ser degradación del desempeño, sesgo, opacidad, uso indebido, falta de aceptación social, incumplimiento regulatorio, daño reputacional o pérdida de confianza. La amplitud de la definición permite a la organización adaptar su marco de análisis a su contexto real. En términos de implementación, esto facilita diseñar controles proporcionales. En clave estratégica, permite entender que la IA afecta objetivos de negocio, legitimidad institucional y responsabilidad ética al mismo tiempo.

## 17. Proceso (3.8)

La norma define proceso como un conjunto de actividades interrelacionadas o que interactúan y que utilizan entradas para proporcionar un resultado previsto. En un SGIA, pensar en procesos es fundamental porque la gestión de IA no puede sostenerse sobre tareas aisladas.

Cada proceso tiene entradas, responsables, criterios, controles y resultados esperados. Esta lógica ayuda a ubicar dónde se toman decisiones, dónde se generan riesgos, dónde se necesita documentación y cómo se produce trazabilidad. En términos operativos, la visión por procesos permite insertar la IA dentro de la gestión real de la organización. En clave de gobernanza, favorece supervisión, comparación y mejora.

## 18. Competencia (3.9)

La competencia es la capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos. Esta definición adquiere especial relevancia en un SGIA porque la eficacia del sistema depende de personas capaces de interpretar, ejecutar y sostener controles con criterio.

No basta con asignar roles. Es necesario asegurar que quienes ocupan esos roles comprendan implicaciones técnicas, normativas, operativas y éticas de la IA. La competencia se refleja en decisiones mejores, documentación más útil, comunicación más precisa y supervisión más efectiva. En consecuencia, esta definición debe entenderse como una condición estructural del sistema, no como un tema secundario de formación.

## 19. Información documentada (3.10)

La norma define información documentada como la información que la organización debe controlar y mantener, junto con el medio que la contiene. Puede estar en cualquier formato y provenir de cualquier fuente. En el SGIA, esta información cumple múltiples funciones a la vez.

Sirve para describir procesos, registrar decisiones, evidenciar controles, sostener revisiones, comparar resultados y preservar memoria organizacional. En clave aplicada, la información documentada se entiende como la columna vertebral de la trazabilidad del sistema. Sin ella, la organización no puede explicar adecuadamente cómo gestiona la IA ni cómo aprende de su experiencia.

## 20. Desempeño (3.11)

La norma define desempeño como un resultado medible, vinculado a hallazgos cuantitativos o cualitativos. En el SGIA, esta definición no debe reducirse al rendimiento técnico del sistema de IA. También abarca el desempeño del propio sistema de gestión.

La organización necesita saber si sus objetivos se cumplen, si sus controles funcionan, si sus riesgos siguen bajo niveles aceptables, si su documentación es útil y si sus mecanismos de revisión realmente aportan valor. Medir desempeño, por tanto, significa evaluar tanto la capacidad del sistema de IA como la eficacia de la estructura que lo gobierna.

## 21. Mejora continua (3.12)

La mejora continua es una actividad recurrente para mejorar el desempeño. Aunque la definición sea breve, su impacto es enorme. El SGIA no puede entenderse como un sistema terminado de una vez y para siempre. Cambian los riesgos, cambian las tecnologías, cambian las expectativas y cambian los contextos de uso.

Por eso, la organización necesita una disciplina de aprendizaje. Debe revisar qué funciona, qué requiere ajuste, qué brechas aparecen y cómo fortalecer la madurez del sistema. Esta definición conecta todas las demás: política, objetivos, procesos, controles, seguimiento y revisión adquieren pleno sentido cuando alimentan un ciclo de evolución.

## 22. Revisión estructurada del sistema

El texto fuente incluye también la definición de auditoría como proceso sistemático, independiente y documentado para obtener y evaluar evidencia objetiva respecto de criterios definidos. En esta versión de autoestudio conviene introducir desde aquí una lectura más pedagógica y menos fiscalizadora: la revisión estructurada del sistema.

Esa lectura no elimina el rigor técnico del término. Lo preserva, pero lo integra en una lógica de aseguramiento y mejora. Para un profesional AIMPC™ o AIGPC™, lo importante no es adoptar una postura punitiva frente al sistema, sino entender cómo la organización utiliza procesos de revisión para identificar brechas, fortalecer decisiones y sostener confianza en la eficacia del SGIA.

### Cierre del módulo 2

Al cierre de este módulo, el participante debe haber comprendido tres cosas. Primero, que la norma tiene una aplicabilidad amplia y no se limita a desarrolladores puros de IA. Segundo, que la referencia normativa a ISO/IEC 22989 es esencial para construir un lenguaje común y coherencia interpretativa. Tercero, que los términos y definiciones no son accesorios: forman la base conceptual sobre la cual se edifican liderazgo, riesgo, controles, seguimiento y mejora.

En la secuencia del documento, este módulo cierra la etapa de precisión conceptual. El siguiente paso consiste en trasladar esa precisión al terreno real de la organización: su contexto, sus partes interesadas, su alcance y la forma concreta en que establecerá el SGIA.

Con esa base, el participante queda preparado para entrar al siguiente módulo, donde el SGIA deja el terreno conceptual inicial y comienza a anclarse en la realidad específica de la organización.

## Módulo 3. Contexto de la organización

### Introducción al módulo

El tercer módulo completa la primera gran parte del documento. Después de comprender los fundamentos de la norma y precisar sus conceptos esenciales, el participante debe situar el SGIA en una organización concreta, con un entorno, unas partes interesadas y unos límites claramente definidos.

Un SGIA no se diseña en abstracto. Se diseña dentro de una organización concreta, con objetivos definidos, riesgos identificados, sistemas específicos y relaciones reales con su entorno. Por eso, la cláusula 4 de ISO/IEC 42001 tiene un valor estructural. Antes de definir controles, la organización necesita entender su contexto. Antes de redactar política, necesita saber qué presiones, expectativas y dependencias condicionan su sistema. Antes de delimitar responsabilidades, necesita comprender cuál es su papel real frente a la IA.

Este módulo debe leerse como el paso en el que la norma obliga a abandonar cualquier aproximación genérica. La gestión de IA no puede construirse con fórmulas copiadas sin reflexión. Requiere interpretar el entorno externo, reconocer factores internos, mapear partes interesadas, decidir el alcance y, a partir de ello, establecer el SGIA como estructura viva de gestión.

La fortaleza de este módulo radica en que conecta operación y gobernanza desde el inicio. Lo operativo aparece en la necesidad de identificar procesos, roles, usos y límites. Lo estratégico surge en la obligación de comprender expectativas sociales, presiones regulatorias, sensibilidad sectorial y decisiones institucionales sobre exposición al riesgo. Esta doble lectura es exactamente la que un profesional senior debe dominar.

## 23. 4.1 Comprensión de la organización y su contexto

La organización determina las cuestiones externas e internas que son relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos de su SGIA. Además, considera si el cambio climático es una cuestión relevante, examina el propósito previsto de los sistemas de IA que desarrolla, proporciona o utiliza, y define sus roles con respecto a esos sistemas.

Esta cláusula es una de las más importantes de toda la norma porque impide construir un SGIA descontextualizado. Una organización no puede implantar un sistema útil si ignora el sector en el que opera, las exigencias regulatorias que la afectan, la sensibilidad social del uso de la IA, su propia cultura interna, sus capacidades reales, su exposición reputacional o la naturaleza específica de los sistemas que utiliza.

Las cuestiones externas pueden incluir legislación, expectativas regulatorias, dinámica competitiva, evolución tecnológica, presión de mercado, estándares sectoriales, contexto geopolítico, sensibilidad pública, exigencias éticas o incluso debates sociales sobre el uso de la IA. Las cuestiones internas pueden abarcar estructura de gobierno, estrategia corporativa, cultura, capacidades técnicas, madurez documental, recursos, experiencia previa con IA, políticas existentes y prioridades del negocio.

La cláusula añade un elemento especialmente relevante: comprender el rol de la organización frente al sistema de IA. Una misma organización puede ser desarrolladora de un sistema, usuaria de otro, integradora de un tercero y cliente de un proveedor externo al mismo tiempo. También puede desempeñar más de un rol respecto del mismo sistema en diferentes etapas de su ciclo de vida. Esta distinción importa porque determina qué responsabilidades son aplicables, qué controles se vuelven críticos y qué profundidad debe tener la supervisión.

En términos operativos, la comprensión del contexto permite adaptar el SGIA a la realidad. En clave estratégica, evita un error costoso: tratar todos los sistemas de IA como si

generaran la misma exposición. No es lo mismo utilizar IA en una función auxiliar de baja criticidad que en decisiones con alto impacto sobre personas, privacidad, seguridad o derechos. El contexto es lo que permite distinguir una situación de la otra.

## 24. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización determina cuáles son las partes interesadas relevantes para el SGIA, cuáles son sus requisitos relevantes y cuáles de esos requisitos se abordan a través del sistema. La norma añade que esas partes interesadas también pueden tener requisitos relacionados con el cambio climático cuando resulte pertinente.

Esta cláusula amplía el horizonte del SGIA más allá de la estructura interna de la organización. Gestionar IA de forma responsable implica reconocer que existen actores con expectativas legítimas sobre cómo se diseña, usa, controla y comunica esa IA. Algunos de esos requisitos serán formales, como los regulatorios o contractuales. Otros serán de carácter reputacional, ético, operativo o social.

El ejercicio no consiste solo en enumerar actores. Requiere determinar cuáles son verdaderamente relevantes y qué exige cada uno al sistema. Un regulador puede esperar trazabilidad, controles y evidencia. Un cliente puede exigir transparencia o capacidad de explicación. Un proveedor crítico puede introducir dependencias que deben supervisarse. Los usuarios internos pueden requerir guía, formación y criterios claros de uso. Las comunidades afectadas pueden demandar sensibilidad frente a posibles impactos.

En términos de implementación, esta cláusula ayuda a traducir expectativas en requisitos operativos. Permite decidir qué controles deben establecerse, qué canales de comunicación serán necesarios, qué información documentada conviene conservar y qué mecanismos de supervisión deben priorizarse. En clave de gobernanza, fortalece legitimidad, porque obliga a la organización a mirar el SGIA no solo desde su conveniencia interna, sino también desde la confianza que debe sostener ante terceros.

## 25. 4.3 Determinación del alcance del sistema de gestión de inteligencia artificial

La organización determina los límites y la aplicabilidad del SGIA para establecer su alcance. Para ello considera las cuestiones externas e internas identificadas en 4.1 y los requisitos relevantes de las partes interesadas identificados en 4.2. Además, el alcance debe mantenerse como información documentada.

Aquí la norma convierte el análisis previo en una decisión estructural. El alcance no es una declaración decorativa. Es el marco que define qué parte de la organización, qué

procesos, qué unidades, qué productos, qué servicios y qué sistemas de IA quedan cubiertos por el SGIA. De su calidad depende, en gran medida, la calidad del sistema completo.

Un alcance demasiado vago genera ambigüedad. Un alcance excesivamente amplio sin recursos suficientes genera fragilidad. Un alcance estrecho mal justificado puede dejar fuera riesgos significativos. Por eso, la determinación del alcance exige criterio. La organización necesita decidir con claridad hasta dónde llega su sistema y cómo justificará esa delimitación.

En términos de implementación, el alcance ordena procesos, responsabilidades, documentación y recursos. En clave estratégica, fija el perímetro de accountability. Delimita dónde la dirección asume formalmente la responsabilidad de gobernar la IA bajo ISO/IEC 42001 y dónde esa responsabilidad aún no se ha incorporado al sistema. En escenarios de certificación, esta precisión es especialmente importante porque condiciona toda la lectura externa del SGIA.

## 26. 4.4 Sistema de gestión de inteligencia artificial

La organización establece, implementa, mantiene y mejora continuamente un SGIA, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de la norma. Esta cláusula resume la esencia de ISO/IEC 42001 y funciona como cierre lógico del módulo de contexto.

Después de comprender el entorno, identificar partes interesadas y delimitar alcance, la organización ya no puede quedarse en el análisis. Debe construir el sistema. Eso implica definir procesos, relaciones, secuencias, responsables, entradas, salidas, mecanismos de control y rutas de mejora. El SGIA debe existir como realidad operativa y no solo como intención declarada.

La referencia a los procesos necesarios y sus interacciones es muy relevante. Un sistema de gestión no se fortalece únicamente por la calidad de cada proceso aislado, sino por la coherencia entre ellos. La política se conecta con los objetivos. Los objetivos con la planificación. La planificación con la operación. La operación con el seguimiento. El seguimiento con la revisión por la dirección. Y la revisión con la mejora. El SGIA solo funciona plenamente cuando esa interacción se diseña y se mantiene de forma consciente.

En clave senior, esta cláusula introduce además una idea poderosa: la organización crea un sistema operativo de gobernanza para la IA. No gestiona casos sueltos. Gestiona una capacidad. Y al hacerlo, vincula dirección, ejecución, control y aprendizaje dentro de una misma arquitectura institucional.

## Integración conceptual del módulo 3

El valor del módulo 3 se entiende mejor cuando se observa su secuencia interna. Primero, la organización interpreta su contexto. Luego identifica a quién debe considerar y qué requisitos resultan relevantes. Después decide el perímetro real del sistema. Finalmente, establece el SGIA como estructura de gestión. Esta progresión no es accidental. Responde a una lógica de construcción.

Sin contexto, el sistema sería genérico. Sin partes interesadas, sería ciego a expectativas externas. Sin alcance, sería ambiguo. Sin sistema, el análisis quedaría sin traducción operativa. Por eso, este módulo constituye el puente entre fundamentos y diseño institucional. Aquí el participante empieza a ver cómo la norma obliga a aterrizar ideas generales dentro de una organización concreta.

## Cierre del módulo 3

Al cierre de este módulo, el participante debe estar en condiciones de responder cuatro preguntas esenciales. Primera: qué factores internos y externos condicionan la gestión de IA en una organización determinada. Segunda: qué partes interesadas son relevantes y qué requisitos introducen. Tercera: cómo debe definirse el alcance del SGIA para que sea claro, proporcional y defendible. Cuarta: qué significa realmente establecer un sistema de gestión de IA con procesos e interacciones estructurados.

Con este punto se cierra la primera parte del documento. Ya existe una base conceptual, terminológica y contextual suficiente. A partir de aquí comienza la segunda parte: la construcción directiva y operativa del sistema, iniciando con el papel de la alta dirección y la arquitectura de liderazgo.

Con estas respuestas, el participante queda listo para avanzar al siguiente bloque de la norma. A partir de aquí, el SGIA ya no se estudia solo como marco general o como sistema contextualizado. Empieza a desplegarse como liderazgo, compromiso, política, responsabilidades y capacidad de conducción desde la alta dirección.

# Módulo 4. Liderazgo

## Introducción al módulo

La segunda parte del documento se concentra en la construcción directiva y operativa del sistema. Su propósito es mostrar cómo el SGIA pasa de estar conceptualmente definido a quedar institucionalmente dirigido, planificado y soportado.

Una vez definido el contexto del SGIA, la norma traslada el foco hacia la conducción institucional del sistema. Este cambio de plano es deliberado. ISO/IEC 42001 no permite que la gestión de la IA quede encapsulada en un área técnica, ni que se trate como una iniciativa periférica desconectada de la dirección estratégica. Al contrario, exige que la alta dirección asuma un papel visible, activo y estructurante.

En términos de autoestudio, este módulo tiene una importancia superior a la que muchas organizaciones le atribuyen en la práctica. Es frecuente que los proyectos de IA se impulsen desde innovación, analítica, tecnología o transformación digital, mientras la dirección mantiene una distancia prudente y delega casi por completo la responsabilidad. La norma corrige esa tendencia. La gestión de la IA requiere liderazgo porque involucra decisiones sobre apetito de riesgo, asignación de recursos, priorización de objetivos, relación con partes interesadas, cultura organizacional y aceptación de impactos. Ninguna de esas decisiones pertenece exclusivamente al nivel técnico.

Por eso, la cláusula 5 debe estudiarse como la entrada formal de la gobernanza en el SGIA. Aquí la IA deja de ser una capacidad observada y pasa a ser una capacidad dirigida. El participante necesita comprender que liderazgo no significa solo apoyo verbal. Significa presencia en la arquitectura del sistema: política, compromiso, integración en procesos de negocio, comunicación, recursos, definición de roles y trazabilidad de responsabilidades.

## 27. Liderazgo

El bloque de liderazgo abre una dimensión crítica dentro del SGIA. La norma establece que la gestión de IA depende de la manera en que la organización dirige, prioriza y respalda el sistema desde los niveles más altos de responsabilidad. Esta afirmación debe interpretarse con amplitud. No se trata únicamente de que la alta dirección conozca la existencia del SGIA. Se trata de que lo reconozca como un componente de la conducción institucional.

En una organización madura, el liderazgo respecto de la IA se expresa en decisiones concretas. Se refleja en la forma en que la dirección fija prioridades, asigna presupuesto, valida políticas, exige información, patrocina mecanismos de control y responde frente a

resultados o incidentes. Bajo esta lógica, la cláusula de liderazgo actúa como un puente entre la estrategia y la operación. Lo que se decide al más alto nivel termina condicionando procesos, controles y comportamientos cotidianos.

En clave AIMPC™ y AIGPC™, este punto tiene gran valor porque demuestra que la IA no puede gobernarse únicamente mediante pericia técnica. Hace falta criterio ejecutivo. El profesional que implementa o supervisa un SGIA debe saber traducir necesidades operativas al lenguaje de la dirección y, al mismo tiempo, convertir expectativas del liderazgo en arquitectura de procesos, controles y métricas.

## 28. 5.1 Liderazgo y compromiso

La alta dirección demuestra liderazgo y compromiso con respecto al SGIA asegurando que la política de IA y los objetivos de IA se establezcan y sean compatibles con la dirección estratégica de la organización. Además, asegura la integración de los requisitos del sistema en los procesos de negocio, la disponibilidad de los recursos necesarios, la comunicación de la importancia de una gestión eficaz de la IA y del cumplimiento de los requisitos del SGIA, así como el logro de los resultados previstos. La norma también exige que la alta dirección dirija y apoye a las personas para contribuir a la eficacia del sistema, promueva la mejora continua y respalde a otros roles relevantes para demostrar liderazgo dentro de sus áreas de responsabilidad.

Esta cláusula contiene, en realidad, un programa completo de responsabilidad directiva. No basta con aprobar el sistema. La alta dirección debe hacerlo compatible con la estrategia institucional. Esa compatibilidad es decisiva, porque un SGIA que no conversa con la dirección del negocio pierde sostenibilidad. Puede existir como proyecto, pero difícilmente se consolidará como sistema.

La referencia a la integración en los procesos de negocio también merece especial atención. La norma aclara que el término “negocio” debe entenderse de forma amplia, es decir, como las actividades fundamentales para la existencia de la organización. Eso significa que el SGIA no puede quedarse aislado en un espacio técnico o documental. Tiene que insertarse allí donde la organización crea valor, toma decisiones, presta servicios, interactúa con clientes, opera procesos críticos o gestiona riesgos relevantes.

Hay otro elemento especialmente relevante: la cultura. El texto base resalta que establecer, fomentar y modelar una cultura de enfoque responsable hacia el uso, desarrollo y gobernanza de los sistemas de IA constituye una manifestación clara del liderazgo de la alta dirección. Este punto merece una lectura detenida. En la práctica, muchas fallas de control no provienen de ausencia total de normas, sino de una cultura que premia velocidad sin trazabilidad, despliegue sin revisión o experimentación sin criterios claros de responsabilidad. La dirección corrige ese sesgo cuando hace visible que la IA no solo debe ser útil, sino también gobernable.

En términos de implementación, 5.1 exige acciones concretas. La alta dirección necesita recibir información periódica, patrocinar el sistema, remover barreras, validar prioridades, exigir seguimiento y crear condiciones para que las áreas responsables cumplan su función. En clave de gobernanza, el propósito es más amplio: demostrar que la IA ha entrado formalmente en el perímetro de la responsabilidad ejecutiva.

## 29. 5.2 Política de IA

La alta dirección establece una política de inteligencia artificial que sea apropiada al propósito de la organización, proporcione un marco para establecer los objetivos de IA, incluya un compromiso de cumplir con los requisitos aplicables y exprese también un compromiso de mejora continua del SGIA. Esta cláusula sitúa a la política como uno de los artefactos centrales del sistema.

La política de IA no debe entenderse como una pieza ceremonial. Su valor reside en que traduce la dirección institucional en un marco formal de actuación. En ella se expresa cómo la organización entiende la IA, qué principios guían su gestión, qué límites reconoce, qué compromisos asume y qué orientación desea dar al sistema en su conjunto. Bien formulada, la política se convierte en un punto de referencia para objetivos, controles, decisiones de tratamiento de riesgo, comunicación y revisión.

En clave pedagógica, conviene subrayar que la política de IA no reemplaza el análisis técnico ni resuelve por sí sola los desafíos operativos. Pero sí establece el tono de la organización. Declara qué se espera del sistema y bajo qué criterios se evaluará su coherencia. En ese sentido, la política cumple una función estratégica: alinea propósito, gobernanza y ejecución.

También resulta relevante que la política sea apropiada al propósito de la organización. Esto implica que no puede redactarse con lenguaje genérico copiado de otra entidad. Debe responder al contexto real, a la naturaleza del uso de IA, a la sensibilidad del sector, al perfil de riesgo y a las expectativas de las partes interesadas. Una política demasiado abstracta aporta poca capacidad de guía. Una política anclada en la realidad institucional, en cambio, fortalece la consistencia del SGIA.

## 30. 5.2 Política de IA: disponibilidad, alineación y comunicación

La política de IA debe mantenerse como información documentada, hacer referencia, cuando corresponda, a otras políticas de la organización, comunicarse dentro de la organización y estar disponible para las partes interesadas relevantes según sea apropiado. La norma remite además a los controles del Anexo A y a la orientación del Anexo B, así como a ISO/IEC 38507 como referencia útil para desarrollar políticas de IA.

Este segundo bloque de 5.2 cobra especial importancia porque evita que la política quede confinada a un documento interno poco conocido. La política gana valor cuando se integra al ecosistema de gobierno de la organización, cuando se articula con otras políticas existentes y cuando llega a quienes deben usarla como referencia real. De nada sirve una política impecable si los responsables de proceso no la conocen, si los controles no se diseñan a partir de ella o si no existe conexión visible con otras estructuras normativas de la organización.

La referencia a otras políticas también es significativa. La IA no opera aislada de calidad, seguridad de la información, privacidad, ética, cumplimiento, continuidad o gobierno corporativo. Por eso, la política de IA necesita dialogar con ese conjunto más amplio. Ese diálogo evita duplicidades, reduce contradicciones y favorece una narrativa institucional coherente.

En clave de gobernanza, la política cumple además una función externa. Dependiendo del contexto, puede ser útil que ciertas partes interesadas conozcan cómo la organización orienta el uso y control de la IA. Esto fortalece confianza, transparencia y legitimidad. No se trata de hacer pública toda la arquitectura del sistema, sino de demostrar que existe una postura institucional clara y trazable.

## 31. 5.3 Roles, responsabilidades y autoridades

La alta dirección asegura que las responsabilidades y autoridades para los roles relevantes se asignen y se comuniquen dentro de la organización. Este requisito parece directo, pero su importancia es enorme. Un SGIA no puede sostenerse si las funciones clave permanecen implícitas, dispersas o ambiguas.

La IA involucra decisiones sobre política, objetivos, riesgos, impactos, controles, seguimiento, remediación y comunicación. Si esas decisiones no tienen responsables definidos, el sistema se vuelve vulnerable a vacíos de coordinación, duplicidades, demoras y ausencia de accountability. Por eso, la norma exige más que una distribución informal de tareas. Exige claridad organizacional.

En la práctica, esta cláusula lleva a la organización a definir quién lidera el SGIA, quién coordina su conformidad con la norma, quién gestiona riesgos, quién supervisa controles, quién conserva la documentación crítica, quién reporta a la dirección y quién participa en la revisión del sistema. No siempre se necesita una estructura compleja, pero sí una asignación visible y comprensible.

En clave de certificación, aquí aparece uno de los signos más claros de madurez. Una organización madura puede explicar de manera sencilla quién hace qué, con qué autoridad y bajo qué criterio de reporte. Una organización inmadura, en cambio, deja esas responsabilidades flotando entre áreas. El SGIA necesita la primera condición, no la segunda.

## 32. 5.3 Roles, responsabilidades y autoridades: conformidad y reporte

La alta dirección asigna la responsabilidad y autoridad necesarias para asegurar que el SGIA cumple con los requisitos de la norma y para informar sobre el desempeño del sistema de gestión de IA a la alta dirección. La referencia al Anexo A y al Anexo B refuerza la necesidad de articular estas funciones con una arquitectura de control más amplia.

Este subbloque profundiza la lógica de accountability. No basta con distribuir tareas generales. El sistema necesita, como mínimo, una capacidad organizacional explícita para dos funciones críticas: asegurar la coherencia técnica y normativa del SGIA, y llevar información fiable sobre su desempeño hacia la dirección. La primera protege la conformidad y la solidez del sistema. La segunda asegura que la dirección no gobierne a ciegas.

En términos operativos, esto puede adoptar distintas formas según el tamaño y complejidad de la organización. En algunos contextos habrá un responsable específico del SGIA. En otros, la función podrá integrarse en una estructura de riesgo, cumplimiento, calidad o gobierno tecnológico. Lo decisivo no es la etiqueta del cargo, sino la claridad de la función. El sistema necesita saber quién vigila su consistencia y quién alimenta a la dirección con información relevante para decidir.

En clave de gobernanza, esta cláusula cierra el módulo de liderazgo de forma contundente. El SGIA no solo requiere intención, política y compromiso. Requiere responsables visibles, autoridad suficiente y rutas de información hacia el más alto nivel. Esa trazabilidad convierte el liderazgo en conducción efectiva.

## Cierre del módulo 4

Al finalizar este módulo, el participante debe reconocer que el liderazgo en ISO/IEC 42001 no es simbólico. La alta dirección define el tono, la prioridad y la legitimidad del SGIA. Establece la política, alinea objetivos, integra el sistema en los procesos fundamentales, asigna recursos, impulsa cultura responsable y distribuye roles con accountability clara.

En la secuencia del documento, este módulo fija la conducción. El siguiente desarrolla el núcleo analítico y decisorio del sistema: la planificación. Allí el liderazgo se traduce en criterios de riesgo, objetivos, impacto y tratamiento.

En síntesis, este módulo enseña una lección decisiva: la IA no puede gobernarse desde la periferia. Requiere centro directivo. Y ese centro directivo se expresa en compromiso visible, política institucional y responsabilidad formalmente asignada.

# Módulo 5. Planificación

## Introducción al módulo

Con el liderazgo ya definido, la norma desplaza el foco hacia el razonamiento operativo del SGIA. Este módulo cumple la función de convertir dirección institucional en decisiones explícitas sobre riesgo, impacto, objetivos y cambio.

Después de comprender el contexto y establecer liderazgo, la organización necesita traducir esa base en decisiones operativas y estratégicas concretas. Esa es la función de la planificación dentro del SGIA. La cláusula 6 marca el momento en que la organización deja de describir su entorno y su compromiso para empezar a estructurar respuesta: identificar riesgos, valorar impactos, definir criterios, seleccionar controles, establecer objetivos y planificar cambios.

En ISO/IEC 42001, planificar no significa simplemente ordenar tareas futuras. Significa construir el razonamiento directivo del sistema. La organización decide qué considera aceptable, qué no puede tolerar, cómo evaluará incertidumbres, qué exposición residual está dispuesta a asumir, cómo traducirá su política en objetivos y cómo sostendrá cambios sin romper la coherencia del SGIA. Esa densidad conceptual explica por qué este módulo es uno de los más extensos y exigentes del programa.

En términos de autoestudio, el participante debe dedicar aquí una atención especial. La cláusula 6 es el verdadero núcleo de decisión del sistema. Contexto y liderazgo preparan el terreno. Planificación define la arquitectura del criterio. Por eso, el lenguaje de este módulo debe conservar profundidad y continuidad, evitando tanto el exceso de síntesis como la fragmentación innecesaria.

## 33. 6 Planificación

La planificación marca el punto en el que la organización convierte el liderazgo, el contexto y la política de IA en acciones concretas. En términos prácticos, es el puente entre intención y sistema operativo. Aquí el SGIA comienza a mostrar cómo responderá a sus riesgos, cómo priorizará oportunidades, qué resultados buscará y cómo preservará consistencia cuando cambien los elementos que lo rodean.

El valor de esta cláusula radica en su capacidad de ordenar decisiones. Una organización que planifica bien no se limita a reaccionar ante incidentes o presiones externas. Anticipa escenarios, define criterios y establece mecanismos para actuar con disciplina. En el terreno de la IA, esto resulta todavía más importante porque los sistemas pueden evolucionar, interactuar con datos variables, generar impactos difíciles de prever y operar en contextos regulatorios en movimiento.

En clave AIMPC™ y AIGPC™, este módulo tiene una fuerza especial porque une gestión y gobernanza de manera explícita. Lo operativo aparece en la necesidad de definir procesos, controles, evaluaciones y planes. Lo estratégico aparece en la obligación de decidir qué nivel de riesgo acepta la organización y qué objetivos justifican el despliegue o el uso de la IA.

## 34. 6.1 Acciones para abordar riesgos y oportunidades

El bloque 6.1 introduce uno de los núcleos estructurales del SGIA: la necesidad de identificar y tratar los riesgos y oportunidades que pueden influir en la capacidad del sistema para alcanzar sus resultados previstos. La norma impide que la organización se limite a una postura reactiva. Exige una lectura dinámica del entorno y del sistema.

Esto significa, en primer lugar, que la organización necesita determinar qué puede desviar sus objetivos de IA, ya sea en sentido adverso o favorable. Los riesgos no deben reducirse a eventos negativos evidentes ni las oportunidades a aspiraciones genéricas. Ambos deben relacionarse con el contexto real del sistema, con sus casos de uso, con los requisitos de partes interesadas y con la forma en que la IA se integra a la operación.

En segundo lugar, implica que identificar no basta. La organización debe traducir esos hallazgos en acciones. Esa transición del análisis a la respuesta constituye uno de los rasgos más maduros de un sistema de gestión. Y en IA, donde las incertidumbres pueden ser técnicas, sociales, regulatorias y éticas al mismo tiempo, esa madurez es especialmente valiosa.

## 35. 6.1.1 General

Al planificar el SGIA, la organización considera las cuestiones identificadas en 4.1 y los requisitos identificados en 4.2, y determina los riesgos y oportunidades que deben abordarse para asegurar que el sistema puede lograr sus resultados previstos, prevenir o reducir efectos no deseados y lograr mejora continua. Esta disposición conecta directamente el análisis del contexto con la toma de decisiones.

La norma deja claro que la planificación no puede hacerse en abstracto. Los riesgos y oportunidades deben surgir del entorno real de la organización, de sus sistemas de IA, de sus partes interesadas y de sus objetivos. Esta conexión evita dos desviaciones comunes: construir matrices de riesgo genéricas, sin relación con la realidad, o tratar la IA solo desde la perspectiva técnica sin considerar sus implicaciones institucionales.

En la práctica, la organización debe preguntarse qué podría afectar la eficacia del SGIA, qué factores podrían comprometer resultados esperados, qué oportunidades podrían fortalecer el sistema y qué decisiones conviene tomar desde el inicio para no dejar al

sistema expuesto a improvisación. El valor estratégico de esta cláusula es alto: convierte el análisis contextual en criterio de dirección.

## 36. 6.1.1 General: criterios de riesgo de IA

La organización establece y mantiene criterios de riesgo de IA que apoyen la distinción entre riesgos aceptables y no aceptables, la realización de evaluaciones de riesgo, el tratamiento de esos riesgos y la evaluación de sus impactos. La norma añade que las consideraciones sobre la cantidad y el tipo de riesgo que una organización está dispuesta a perseguir o retener pueden encontrarse en ISO/IEC 38507 e ISO/IEC 23894.

Este requisito es fundamental porque fija la base de comparación del sistema. Sin criterios de riesgo, la organización no puede evaluar de manera consistente. Cada equipo terminaría interpretando de forma distinta qué es grave, qué es tolerable y qué exige escalamiento. Con criterios claros, en cambio, las decisiones ganan trazabilidad y coherencia.

Además, los criterios de riesgo cumplen una función de gobernanza muy relevante: traducen el apetito y la tolerancia institucional al lenguaje del SGIA. No son únicamente una variable metodológica. Son una expresión de la postura organizacional frente a la incertidumbre. Por ello, deben ser comprensibles, justificables y lo bastante estables como para orientar decisiones repetidas en distintos contextos.

## 37. 6.1.1 General: determinación de riesgos y oportunidades según dominio y contexto

La organización determina los riesgos y oportunidades de acuerdo con el dominio y el contexto de aplicación del sistema de IA, el uso previsto y el contexto externo e interno ya identificado. La norma aclara que pueden existir varios sistemas de IA dentro del alcance del SGIA y que la determinación debe hacerse para cada sistema o para agrupaciones de sistemas cuando resulte apropiado.

Esta precisión evita una lectura genérica del riesgo. No todos los sistemas de IA tienen el mismo propósito, la misma criticidad ni la misma sensibilidad. Un sistema que automatiza una tarea administrativa de bajo impacto no debe analizarse igual que uno que influye en decisiones con alto efecto sobre personas, operaciones esenciales o compromisos regulatorios. El SGIA necesita, por tanto, una lógica de proporcionalidad.

En términos de implementación, esto exige analizar cada sistema según su dominio, su uso previsto, su interacción con personas, el tipo de datos involucrados, la sensibilidad del entorno y la criticidad del resultado. En clave estratégica, ayuda a la organización a asignar recursos y nivel de control donde realmente importan, evitando tanto la sobrerregulación innecesaria como la subestimación de exposiciones relevantes.

## 38. 6.1.1 General: planificación de acciones

La organización planifica las acciones para abordar los riesgos y oportunidades identificados, así como la forma de integrar e implementar dichas acciones en los procesos del SGIA y de evaluar la eficacia de esas acciones. Con esta exigencia, la norma da un paso decisivo: obliga a pasar del análisis a la ejecución.

Una vez identificados riesgos y oportunidades, la organización debe convertirlos en decisiones concretas. Eso implica determinar qué controles serán necesarios, qué procesos deberán ajustarse, qué recursos harán falta, qué seguimiento será apropiado y cómo se verificará si la acción adoptada fue suficiente. Este enfoque evita que la gestión del riesgo quede atrapada en matrices o reportes sin traducción operativa.

En clave senior, aquí se observa uno de los grandes diferenciales de un SGIA maduro: su capacidad de integrar decisiones de riesgo dentro de la operación real. Un sistema inmaduro registra riesgos. Un sistema maduro los convierte en gestión activa.

## 39. 6.1.1 General: información documentada sobre acciones

La organización conserva información documentada sobre las acciones tomadas para identificar y abordar riesgos y oportunidades de IA. La referencia a ISO/IEC 23894 recuerda que la gestión del riesgo debe adaptarse al contexto y a las actividades reales de la organización.

La documentación en este punto no es burocracia. Es memoria de decisión. Permite reconstruir qué riesgos fueron identificados, qué oportunidades se consideraron, cómo se justificaron las prioridades y qué acciones se adoptaron. Sin esa trazabilidad, la organización pierde continuidad, dificulta la revisión futura y reduce su capacidad para explicar por qué gobierna la IA de una determinada manera.

En clave de certificación, esta información documentada es especialmente valiosa porque demuestra consistencia. No solo acredita que hubo análisis. También evidencia que hubo criterio y que el criterio quedó preservado.

## 40. 6.1.1 General: adaptación sectorial del concepto de riesgo

La norma aclara que la forma de definir el riesgo puede variar entre sectores e industrias, y que corresponde a la organización adoptar una visión ajustada a su contexto, pudiendo considerar definiciones sectoriales cuando sean pertinentes. Este matiz es importante porque combina flexibilidad con rigor.

ISO/IEC 42001 no impone una lectura rígida y única del riesgo. Reconoce que un entorno financiero, sanitario, industrial, educativo o gubernamental puede trabajar con lenguajes

sectoriales diferentes. Sin embargo, esa flexibilidad no autoriza arbitrariedad. La organización debe justificar la perspectiva adoptada y mantener consistencia interna.

En términos de implementación, esto permite diseñar un sistema más realista. En clave de gobernanza, asegura que el SGIA dialogue con el ecosistema regulatorio y operativo del sector en el que la organización actúa.

## 41. 6.1.2 Evaluación de riesgos de IA

La organización define y establece un proceso de evaluación de riesgos de IA que esté informado y alineado con la política y con los objetivos de IA. Este punto es decisivo porque evita que la evaluación de riesgos se convierta en un ejercicio aislado o puramente técnico.

La evaluación de riesgos debe responder a la dirección declarada por la política y a los resultados que la organización busca lograr con su SGIA. De este modo, el riesgo no se analiza en abstracto. Se analiza en función del propósito, la estrategia y las prioridades institucionales. Esa alineación fortalece la coherencia del sistema y evita que el análisis se transforme en una práctica desconectada del resto del marco de gestión.

## 42. 6.1.2 Evaluación de riesgos de IA: consistencia y comparabilidad

El proceso de evaluación de riesgos debe diseñarse de tal manera que evaluaciones repetidas produzcan resultados consistentes, válidos y comparables. Además, debe identificar riesgos que ayuden o impidan lograr los objetivos de IA.

Este requisito introduce una expectativa metodológica muy alta. El SGIA necesita una forma de evaluación que no dependa excesivamente de juicios cambiantes, intuiciones individuales o criterios inestables. La comparabilidad importa porque permite observar evolución, justificar decisiones y sostener revisiones posteriores con base en información consistente.

La mención a riesgos que ayudan o impiden el logro de objetivos también amplía la mirada. La gestión del riesgo en IA no se limita a frenar problemas. Además ayuda a reconocer factores que fortalecen o debilitan la capacidad del sistema para producir valor. Esta visión resulta especialmente útil para una lectura estratégica del SGIA.

## 43. 6.1.2 Evaluación de riesgos de IA: análisis de consecuencias, probabilidad y nivel de riesgo

La organización analiza los riesgos de IA para evaluar las posibles consecuencias para la organización, los individuos y las sociedades en caso de materialización, evaluar la

probabilidad realista cuando resulte aplicable y determinar los niveles de riesgo correspondientes.

Aquí la norma introduce una de sus características más distintivas. La evaluación de riesgos en IA no se limita al daño organizacional. Además considera consecuencias sobre personas y sociedad. Esta amplitud convierte al SGIA en un sistema especialmente sensible a la naturaleza socio-técnica de la IA.

En la práctica, la organización necesita examinar qué podría ocurrir, a quién podría afectar, con qué intensidad y con qué probabilidad razonable. Ese análisis debe ser suficientemente robusto como para distinguir entre exposiciones menores y situaciones que exigen decisiones más severas de control, supervisión o rediseño.

## 44. 6.1.2 Evaluación de riesgos de IA: comparación con criterios y priorización

La organización evalúa los riesgos de IA comparando los resultados del análisis con los criterios establecidos en 6.1.1 y prioriza los riesgos evaluados para su tratamiento. Este paso convierte el análisis en una base real para decidir.

La comparación con criterios evita respuestas improvisadas. La organización no trata riesgos por intuición, presión del momento o percepción subjetiva. Los trata con base en una referencia previamente establecida. De esta forma, puede decidir qué riesgos son aceptables, cuáles requieren tratamiento prioritario y cuáles deben escalarse hacia instancias de mayor decisión.

## 45. 6.1.2 Evaluación de riesgos de IA: información documentada

La organización conserva información documentada sobre el proceso de evaluación de riesgos. La norma añade que, al evaluar consecuencias, puede utilizar una evaluación de impacto del sistema de IA según lo indicado en 6.1.4.

Este requisito refuerza la trazabilidad del análisis. No solo importa el resultado final. También importa cómo se definió el proceso, qué variables se consideraron y con qué lógica se asignaron niveles de riesgo. Además, la referencia a la evaluación de impacto anticipa una relación clave dentro del SGIA: riesgo e impacto no operan de manera separada. Se alimentan mutuamente.

## 46. 6.1.3 Tratamiento de riesgos de IA

Teniendo en cuenta los resultados de la evaluación de riesgos, la organización define un proceso de tratamiento de riesgos de IA para seleccionar opciones apropiadas de tratamiento. Esta cláusula marca el paso desde el diagnóstico hacia la intervención.

Tratar el riesgo significa decidir cómo responder a él. En algunos casos será suficiente con controles ya existentes. En otros, la organización tendrá que diseñar medidas nuevas, reforzar supervisión, redefinir procesos, limitar usos, establecer condiciones más estrictas o incluso reconsiderar la viabilidad del sistema en determinados contextos. El tratamiento exige proporcionalidad. No todas las situaciones requieren la misma respuesta.

## 47. 6.1.3 Tratamiento de riesgos de IA: controles y comparación con el Anexo A

La organización determina todos los controles necesarios para implementar las opciones elegidas y compara esos controles con los del Anexo A para verificar que no se haya omitido ningún control necesario. La norma recuerda que el Anexo A proporciona controles de referencia para cumplir objetivos organizacionales y abordar riesgos relacionados con el diseño y uso de sistemas de IA.

Este punto es central porque conecta directamente la gestión del riesgo con la arquitectura de control. El Anexo A no sustituye el juicio organizacional, pero actúa como referencia estructurada para verificar suficiencia. Gracias a esta comparación, la organización puede detectar omisiones y justificar mejor por qué selecciona unos controles y no otros.

## 48. 6.1.3 Tratamiento de riesgos de IA: controles adicionales

La organización considera los controles del Anexo A que sean relevantes para la implementación del tratamiento y también identifica si son necesarios controles adicionales más allá de los incluidos en ese anexo. Esta flexibilidad es una fortaleza del SGIA.

No todos los entornos tienen las mismas obligaciones, ni todos los riesgos quedan cubiertos por un conjunto estándar de controles. La organización puede necesitar medidas adicionales debido a requisitos regulatorios, criticidad sectorial, sensibilidad de los datos, dependencia de terceros o impacto potencial sobre personas. La norma permite y exige esa adaptación cuando resulte necesaria.

## 49. 6.1.3 Tratamiento de riesgos de IA: orientación del Anexo B

La organización considera la orientación del Anexo B para la implementación de los controles determinados. La norma aclara que los controles elegidos incluyen implícitamente objetivos de control y que tanto esos objetivos como los controles pueden complementarse cuando el contexto lo exija.

El valor del Anexo B radica en que ayuda a traducir la selección de controles en decisiones de implementación más concretas. No basta con decidir que un control existe. Es

necesario comprender cómo operará, qué evidencias generará, qué responsables tendrá y cómo se integrará con procesos y recursos ya existentes.

## 50. 6.1.3 Tratamiento de riesgos de IA: Declaración de Aplicabilidad

La organización produce una Declaración de Aplicabilidad que contenga los controles necesarios y proporcione justificación para la inclusión y exclusión de controles. Esta declaración, conocida comúnmente como SoA, es uno de los artefactos más importantes del SGIA.

Su valor no está solo en enumerar controles. Su valor reside en demostrar la lógica con la que la organización relaciona riesgos, decisiones de tratamiento, objetivos de control y justificaciones de inclusión o exclusión. La SoA se convierte así en un puente entre el análisis y la arquitectura de control. Y en clave de gobernanza, funciona como evidencia clara de que las decisiones no se toman al azar.

## 51. 6.1.3 Tratamiento de riesgos de IA: plan y aceptación del riesgo residual

La organización formula un plan de tratamiento de riesgos de IA y obtiene la aprobación de la dirección designada tanto para el plan como para la aceptación de los riesgos residuales. Este requisito cierra el ciclo de decisión con una señal de gobierno muy clara.

El riesgo residual no puede asumirse de manera tácita o accidental. Debe ser aceptado conscientemente por una instancia con autoridad suficiente. Esta exigencia eleva la calidad del sistema porque obliga a explicitar la exposición remanente y a vincularla con el apetito de riesgo institucional.

## 52. 6.1.3 Tratamiento de riesgos de IA: alineación, documentación y comunicación

Los controles necesarios se alinean con los objetivos establecidos en 6.2, se mantienen como información documentada, se comunican dentro de la organización y se ponen a disposición de partes interesadas cuando corresponda. Aquí la norma recuerda que el control no es un elemento aislado.

Un control solo aporta valor real cuando tiene sentido dentro del marco de objetivos del SGIA, cuando queda formalizado y cuando es conocido por quienes deben aplicarlo o supervisarlo. De lo contrario, existe en el papel pero no en la operación.

## 53. 6.1.3 Tratamiento de riesgos de IA: trazabilidad del proceso

La organización conserva información documentada sobre el proceso de tratamiento de riesgos de IA. Esta trazabilidad permite reconstruir decisiones, revisar la eficacia de los tratamientos elegidos y sostener aprendizaje acumulativo dentro del sistema.

## 54. 6.1.4 Evaluación de impacto del sistema de IA

La organización define un proceso para evaluar las posibles consecuencias para individuos, grupos de individuos y sociedades que pueden resultar del desarrollo, provisión o uso de sistemas de IA. Esta cláusula amplía el foco del SGIA y le da una profundidad distintiva.

La evaluación de impacto no sustituye la evaluación de riesgo, pero la complementa. Introduce una mirada específica sobre efectos potenciales, especialmente aquellos que pueden afectar a personas o grupos de manera directa o indirecta. Esto hace visible la necesidad de una gestión responsable y sensible al contexto social del sistema.

## 55. 6.1.4 Evaluación de impacto del sistema de IA: uso previsto y uso indebido previsible

La evaluación de impacto determina las posibles consecuencias que el despliegue, el uso previsto y el uso indebido previsible de un sistema de IA pueden tener sobre individuos, grupos y sociedades. Esta amplitud preventiva resulta esencial.

No basta con examinar el escenario ideal de uso. La organización también debe preguntarse cómo podría utilizarse indebidamente el sistema de manera razonablemente previsible y qué efectos se derivarían de ello. Esta reflexión fortalece la responsabilidad organizacional y mejora la calidad del análisis previo al despliegue o durante la operación.

## 56. 6.1.4 Evaluación de impacto del sistema de IA: contexto técnico, social y jurisdiccional

La evaluación de impacto tiene en cuenta el contexto técnico y social específico en el que se despliega el sistema, así como las jurisdicciones aplicables. Un mismo sistema puede producir consecuencias muy distintas según el entorno de uso, el tipo de usuarios, la cultura, la sensibilidad del dominio o el marco regulatorio.

Por eso, el análisis de impacto debe situarse siempre en una realidad concreta. Esta contextualización fortalece la gobernanza, porque evita decisiones abstractas y obliga a considerar dónde, cómo y sobre quién operará la IA.

## 57. 6.1.4 Evaluación de impacto del sistema de IA: documentación y disponibilidad

El resultado de la evaluación de impacto se documenta y, cuando sea apropiado, puede ponerse a disposición de partes interesadas relevantes definidas por la organización. La documentación aporta trazabilidad. La disponibilidad, cuando corresponde, puede fortalecer transparencia y confianza.

## 58. 6.1.4 Evaluación de impacto del sistema de IA: relación con la evaluación de riesgos

La organización considera los resultados de la evaluación de impacto dentro de la evaluación de riesgos. La norma añade que, en algunos contextos, como sistemas críticos para seguridad o privacidad, pueden requerirse evaluaciones de impacto específicas por disciplina como parte de las actividades generales de gestión del riesgo.

Esta conexión es especialmente valiosa porque evita que impacto y riesgo se traten como ejercicios separados. Cuando ambos procesos dialogan, la calidad del análisis mejora y las decisiones de tratamiento ganan profundidad.

## 59. 6.2 Objetivos de IA y planificación para lograrlos

La organización establece objetivos de IA en funciones y niveles relevantes. Esta disposición convierte la política y el análisis previo en resultados esperados. Los objetivos son la forma en que la organización traduce intención en dirección concreta.

Un SGIA sin objetivos claros corre el riesgo de quedar atrapado en buenas intenciones. Un SGIA con objetivos bien construidos, en cambio, puede asignar responsabilidades, movilizar recursos, medir avance y sostener decisiones con criterio. En la práctica, los objetivos ayudan a ordenar la gestión de la IA. En clave de gobernanza, permiten mostrar qué valor busca la organización y bajo qué condiciones espera alcanzarlo.

## 60. 6.2 Objetivos de IA y planificación para lograrlos: coherencia, medición y seguimiento

Los objetivos de IA son coherentes con la política, medibles cuando sea practicable, tienen en cuenta los requisitos aplicables y son monitoreados. Estas condiciones definen la calidad mínima de un objetivo útil.

Un objetivo que no se puede seguir, que no conversa con la política o que ignora requisitos relevantes tiene poco valor dentro del SGIA. En cambio, un objetivo bien formulado se convierte en una referencia real para la acción y la evaluación.

## 61. 6.2 Objetivos de IA y planificación para lograrlos: comunicación, actualización y documentación

Los objetivos de IA se comunican, se actualizan según corresponda y se mantienen como información documentada. Con ello, la norma recuerda que los objetivos no deben quedar confinados a un ejercicio inicial de planeación.

Deben ser conocidos por quienes participan en su cumplimiento, revisarse cuando cambie el contexto y quedar disponibles como referencia de gestión. Solo así dejan de ser declaraciones estáticas y se convierten en instrumentos vivos del SGIA.

## 62. 6.2 Objetivos de IA y planificación para lograrlos: despliegue operativo

Al planificar cómo lograr sus objetivos de IA, la organización determina qué se hará, qué recursos se requerirán, quién será responsable, cuándo se completará y cómo se evaluarán los resultados. Este requisito convierte el objetivo en un compromiso ejecutable.

La norma exige pasar de la meta al plan. Esa transición fortalece trazabilidad y disciplina. También permite conectar objetivos con recursos, tiempos, responsables y métricas de resultado.

## 63. 6.2 Objetivos de IA y planificación para lograrlos: apoyo de anexos

La norma indica que el Anexo C presenta una lista no exhaustiva de objetivos relacionados con la gestión de riesgos y que los Anexos A y B aportan objetivos de control, controles y orientación para identificar objetivos de desarrollo y uso responsable de sistemas de IA. Este recordatorio ayuda a ampliar criterio y a diseñar un SGIA más maduro.

## 64. 6.3 Planificación de cambios

Cuando la organización determina la necesidad de cambios en el SGIA, esos cambios se llevan a cabo de manera planificada. Aunque breve, esta cláusula tiene gran importancia.

El SGIA no es estático. Cambia cuando evolucionan sistemas, procesos, obligaciones, riesgos o prioridades estratégicas. La norma exige que esos cambios no se gestionen de forma improvisada. Deben evaluarse, ordenarse y ejecutarse con disciplina para preservar coherencia, trazabilidad y eficacia.

## Cierre del módulo 5

Al concluir este módulo, el participante debe comprender que la planificación en ISO/IEC 42001 no es un trámite. Es el corazón analítico y decisorio del SGIA. Aquí se determinan

criterios de riesgo, se evalúan consecuencias, se definen tratamientos, se seleccionan controles, se construye la Declaración de Aplicabilidad, se establecen objetivos y se ordenan cambios.

Dentro de la macroestructura del documento, este módulo convierte la dirección en criterio. El módulo siguiente añade la condición de viabilidad: recursos, competencia, comunicación y documentación para que lo planificado pueda sostenerse en la práctica.

En síntesis, este módulo enseña cómo la organización transforma contexto y liderazgo en criterio operativo y postura de gobernanza. La IA deja de ser una capacidad que simplemente existe dentro de la organización. Pasa a ser una capacidad deliberadamente dirigida bajo parámetros explícitos de riesgo, impacto, control y resultado.

# Módulo 6. Soporte

## Introducción al módulo

El tercer módulo de esta segunda parte responde a una pregunta crucial: con qué capacidades reales sostendrá la organización el sistema que ya ha decidido construir. Su función es cerrar la arquitectura de diseño del SGIA y prepararla para entrar en funcionamiento.

Después de definir contexto, liderazgo y planificación, la organización necesita asegurar que el SGIA puede funcionar en condiciones reales. Esa es la finalidad de la cláusula 7. El soporte reúne los elementos habilitadores del sistema: recursos, competencia, concienciación, comunicación e información documentada.

Este módulo tiene una importancia práctica enorme. Muchas implementaciones fracasan no porque la organización desconozca los requisitos de la norma, sino porque intenta sostener el sistema sin capacidades suficientes. Se redactan políticas, se aprueban matrices, se diseñan controles, pero faltan personas preparadas, canales de comunicación claros, recursos asignados o trazabilidad documental. El soporte corrige ese vacío. Convierte el SGIA en una capacidad operable.

En clave de autoestudio, aquí el participante debe reconocer que ningún sistema de gestión vive solo de decisiones estratégicas. Necesita habilitadores concretos. La norma no acepta una gobernanza puramente declarativa. Exige que la organización cuente con medios reales para ejecutar, mantener y mejorar el sistema.

## 65. 7 Soporte

La cláusula de soporte reúne los elementos que permiten que el SGIA funcione de forma real y sostenida. Después de definir liderazgo, riesgos, impactos y objetivos, la organización debe asegurar que dispone de recursos, capacidades, mecanismos de comunicación y documentación suficiente para implementar y mantener el sistema.

Este punto merece leerse como una verificación de realidad. La pregunta ya no es solo qué quiere hacer la organización con la IA o cómo la quiere gobernar. La pregunta es si cuenta con los medios para hacerlo con consistencia. En clave de certificación, este módulo separa las implementaciones teóricas de las implementaciones maduras.

## 66. 7.1 Recursos

La organización determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGIA. La norma remite además al Anexo A y al Anexo B en materia de recursos para IA.

Este requisito subraya que el SGIA necesita una base material y organizacional para existir. Los recursos pueden incluir personal especializado, tiempo de dedicación, presupuesto, herramientas, infraestructura tecnológica, acceso a asesoría, sistemas de documentación, mecanismos de coordinación y capacidades de supervisión. Sin estos elementos, el SGIA difícilmente podrá pasar del diseño a la práctica.

En términos de implementación, asignar recursos significa hacer posible la ejecución. En clave de gobernanza, significa demostrar compromiso real. La dirección no muestra seriedad frente a la IA solo mediante discursos o políticas. La demuestra cuando dota al sistema de medios suficientes para operar y mejorar.

## 67. 7.2 Competencia

La organización determina la competencia necesaria de las personas que realizan trabajos bajo su control y que afectan su desempeño en IA. Esta disposición sitúa a las personas en el centro del sistema.

La IA no se gestiona únicamente con documentos ni con herramientas. Se gestiona con personas capaces de interpretar requisitos, comprender riesgos, aplicar controles, documentar decisiones, operar procesos y ejercer juicio. Por eso, la organización necesita identificar qué competencias requiere según sus roles, procesos y sistemas de IA. Algunas serán técnicas. Otras serán jurídicas, de cumplimiento, de gestión del riesgo, de ética aplicada, de supervisión o de coordinación interfuncional.

## 68. 7.2 Competencia: desarrollo y evaluación de la competencia

La organización asegura que estas personas sean competentes sobre la base de educación, formación o experiencia apropiada y, cuando sea aplicable, toma acciones para adquirir la competencia necesaria y evalúa la eficacia de las acciones adoptadas.

Esta cláusula introduce una lógica de mejora muy clara. La competencia no se presume. Se construye y se verifica. La organización necesita detectar brechas, decidir cómo cerrarlas y comprobar si la acción efectivamente fortaleció la capacidad requerida. Las respuestas pueden incluir formación, mentoría, reasignación de funciones, incorporación de talento o apoyo especializado.

En clave estratégica, este requisito refuerza que la competencia es una capacidad crítica del SGIA. Una organización puede tener excelentes controles en el papel y, aun así, fallar si las personas que deben ejecutarlos carecen de comprensión suficiente.

## 69. 7.2 Competencia: evidencia documentada

La información documentada apropiada se mantiene como evidencia de la competencia. Este requisito aporta trazabilidad a la gestión del talento dentro del SGIA.

La organización debe poder demostrar qué competencias consideró necesarias, qué acciones emprendió para desarrollarlas y con qué base afirma que una persona es competente para su rol. Esta evidencia favorece continuidad, revisión y capacidad de ajuste. También permite que la dirección comprenda si el sistema dispone del capital humano que necesita para sostener sus resultados.

## 70. 7.2 Competencia: orientación adicional del Anexo B

La norma añade que la orientación de implementación para recursos humanos se proporciona en el Anexo B y aclara que las acciones aplicables pueden incluir provisión de formación, mentoría, reasignación de personas actualmente empleadas o contratación o subcontratación de personas competentes. Este complemento resulta útil porque recuerda que la competencia puede fortalecerse por distintas vías y que la organización debe elegir la más adecuada según su contexto.

## 71. 7.3 Concienciación

Las personas que realizan trabajos bajo el control de la organización son conscientes de la política de IA. Este requisito pone el foco en una dimensión que suele subestimarse: la conciencia organizacional.

No basta con que la política exista. Tiene que ser conocida y comprendida por quienes influyen en el desempeño del SGIA. Cuando esto ocurre, el sistema gana coherencia cultural. Las decisiones cotidianas se alinean mejor con la intención institucional y disminuye la probabilidad de que el SGIA quede reducido a una capa documental sin efecto en la práctica.

## 72. 7.3 Concienciación: contribución e implicaciones del incumplimiento

Las personas bajo el control de la organización además son conscientes de su contribución a la eficacia del SGIA, incluidos los beneficios de mejorar el desempeño de la IA, y de las implicaciones de no cumplir los requisitos del sistema.

Esta disposición amplía la concienciación más allá del conocimiento de la política. La norma espera que las personas entiendan cómo su trabajo afecta el sistema y por qué su papel importa. Esto distribuye responsabilidad y fortalece cultura. También ayuda a que la gestión de la IA no dependa exclusivamente de un pequeño grupo de especialistas.

## 73. 7.4 Comunicación

La organización determina las comunicaciones internas y externas relevantes para el SGIA, incluyendo qué comunicará y cuándo lo comunicará. La comunicación dentro del sistema no es una función auxiliar. Es un mecanismo de coordinación, transparencia y respuesta.

A través de la comunicación, la organización articula expectativas, informa prioridades, notifica cambios, coordina incidentes, comparte decisiones y mantiene alineadas a las partes relevantes. En IA, donde distintos equipos pueden intervenir sobre datos, modelos, despliegues, monitoreo y control, una comunicación débil se traduce rápidamente en pérdida de coherencia.

## 74. 7.4 Comunicación: destinatarios y medios

La organización determina también con quién comunicará y cómo lo hará. No toda información debe circular del mismo modo ni llegar a los mismos destinatarios. La organización necesita definir audiencias, sensibilidad, oportunidad y canales apropiados.

Este criterio fortalece la gobernanza del SGIA porque evita desorden informativo. Permite que la información relevante llegue a quien debe actuar sobre ella, con el nivel de detalle adecuado y a través del mecanismo más útil para el contexto.

## 75. 7.5 Información documentada

La cláusula de información documentada introduce uno de los soportes más importantes del SGIA: la necesidad de controlar y mantener la información que permite demostrar cómo funciona el sistema, cómo se toman decisiones y cómo se sostiene la trazabilidad de procesos y resultados.

En la práctica, la información documentada es la memoria del SGIA. Sin ella, la organización pierde continuidad, dificulta el seguimiento, complica la revisión por la dirección y reduce su capacidad para defender la coherencia de sus decisiones. En un sistema que gestiona riesgo, impacto y control de IA, esta memoria es especialmente crítica.

## 76. 7.5.1 General

El SGIA incluye la información documentada requerida por la norma y también la que la propia organización determine como necesaria para la eficacia del sistema. Esta disposición evita una interpretación mínima y rígida.

La organización no debe limitarse a producir solo lo estrictamente exigido. Además necesita decidir qué documentación adicional requiere su realidad específica. Esto permite adaptar el sistema a su tamaño, complejidad, sensibilidad sectorial y madurez organizacional. La clave está en conservar suficiente información para sostener eficacia, control y mejora, sin caer en sobrecarga documental innecesaria.

## 77. 7.5.1 General: extensión variable de la documentación

La norma aclara que la extensión de la información documentada puede diferir entre organizaciones debido al tamaño, al tipo de actividades, procesos, productos y servicios, a la complejidad de las interacciones y a la competencia de las personas. Este matiz resulta muy valioso.

No todas las organizaciones requieren el mismo volumen documental. La proporcionalidad sigue siendo un principio rector. Sin embargo, esa proporcionalidad debe justificarse. Menos documentación no siempre significa mejor sistema. Más documentación tampoco garantiza madurez. Lo importante es la suficiencia y utilidad de la información documentada frente al contexto del SGIA.

## 78. 7.5.2 Creación y actualización de información documentada

Al crear y actualizar información documentada, la organización asegura una identificación y descripción apropiadas, por ejemplo mediante título, fecha, autor o número de referencia. Esta exigencia parece básica, pero cumple una función esencial de orden y trazabilidad.

Un documento mal identificado pierde utilidad rápidamente. La organización necesita saber qué documento es, a qué versión corresponde, quién lo emitió y cómo se relaciona con otros artefactos del sistema. Esa disciplina fortalece control, recuperación y confianza en la información utilizada.

## 79. 7.5.2 Creación y actualización de información documentada: formato, medio, revisión y aprobación

La organización asegura además el formato apropiado, el medio adecuado y la revisión y aprobación para idoneidad y adecuación. Esto completa la lógica de calidad documental.

No basta con que la información exista. Debe ser comprensible, estar en un formato útil para quienes la necesitan y haber pasado por una revisión que confirme su pertinencia. Solo entonces puede funcionar como soporte real del SGIA.

## 80. 7.5.3 Control de la información documentada

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

Esta cláusula resume el equilibrio central del control documental: disponibilidad y protección. La organización necesita que la información llegue a quien la requiere, pero además debe protegerla frente a accesos, modificaciones o exposiciones inapropiadas. En un SGIA, donde la documentación puede involucrar riesgos, impactos, decisiones sensibles o relaciones con terceros, ese equilibrio es especialmente delicado.

## 81. 7.5.3 Control de la información documentada: distribución, acceso, recuperación, uso y preservación

La organización aborda actividades como distribución, acceso, recuperación, uso, almacenamiento y preservación, incluida la preservación de la legibilidad. Este requisito asegura que la documentación siga siendo utilizable con el tiempo.

No sirve conservar archivos que no pueden recuperarse, entenderse o utilizarse cuando hacen falta. La documentación del SGIA debe permanecer viva, accesible y funcional como apoyo para decisiones, revisiones y mejora.

## 82. 7.5.3 Control de la información documentada: cambios, retención y disposición

La organización aborda también el control de cambios, por ejemplo mediante control de versiones, así como la retención y disposición de la información documentada. Aquí la norma protege continuidad e integridad del sistema.

Sin una gestión adecuada de versiones, la organización puede operar con documentos obsoletos, criterios contradictorios o decisiones ya superadas. Y sin criterios de retención y disposición, puede perder trazabilidad o acumular información sin valor práctico. El control del ciclo de vida documental es, por tanto, un componente real del SGIA.

## 83. 7.5.3 Control de la información documentada: información de origen externo

La información documentada de origen externo que la organización determine como necesaria para la planificación y operación del SGIA se identifica y controla según

corresponda. Además, el acceso puede implicar decisiones sobre permiso de visualización y autoridad de modificación.

Este punto cobra especial importancia porque recuerda que el SGIA no depende solo de documentos internos. Además puede requerir normas externas, lineamientos regulatorios, especificaciones de proveedores, documentación contractual o referencias técnicas. Esa información influye sobre la planificación y la operación del sistema, por lo que también debe quedar bajo control.

## Cierre del módulo 6

Al concluir este módulo, el participante debe comprender que el soporte es la capa habilitadora del SGIA. Aquí la organización demuestra si posee recursos suficientes, personas competentes, conciencia organizacional, comunicación ordenada y documentación trazable. Sin estos elementos, liderazgo y planificación quedan debilitados. Con ellos, el SGIA gana capacidad real de ejecución y sostenimiento.

Con este punto termina la segunda parte del documento. El sistema ya cuenta con dirección, criterio y soporte. La tercera parte mostrará si todo ello se traduce en funcionamiento verificable, evaluación rigurosa y mejora continua.

En síntesis, este módulo deja una lección muy clara: la gestión responsable de la IA no se sostiene solo en decisiones correctas. Se sostiene en capacidades organizacionales concretas que permiten ejecutar, demostrar, revisar y mejorar esas decisiones en el tiempo.

# Módulo 7. Operación

## Introducción al módulo

La tercera parte del documento entra en la fase de verificación práctica del SGIA. Ya no basta con haberlo diseñado correctamente. Ahora corresponde observar cómo se ejecuta, cómo se revisa y cómo evoluciona.

Hasta este punto, el SGIA ya cuenta con fundamentos, contexto, liderazgo, criterios de planificación y elementos de soporte. La cláusula 8 marca el momento en que todo ese diseño se pone a prueba en la realidad operativa. Aquí la norma exige que la organización planifique, implemente y controle efectivamente los procesos necesarios para cumplir los requisitos del sistema y para ejecutar las acciones definidas frente a riesgos, impactos y objetivos.

Esta transición es decisiva. Una organización puede haber redactado una política excelente, puede haber definido con precisión su contexto y puede incluso haber formulado criterios de riesgo robustos. Sin embargo, nada de eso garantiza por sí solo que el SGIA funcione. La eficacia del sistema se verifica cuando los controles operan, cuando los procesos se ejecutan bajo criterios definidos, cuando los cambios se gobiernan con disciplina y cuando la relación con terceros no rompe la coherencia del marco interno.

En términos de autoestudio, el módulo de operación debe leerse como el punto de inflexión entre arquitectura y desempeño real. Lo que antes se presentaba como compromiso, planificación o soporte ahora debe materializarse en funcionamiento verificable. Por eso, esta parte de la norma tiene un peso especial para perfiles AIMPC™, orientados a implantación, y también para perfiles AIGPC™, porque muestra si la estructura de gobernanza realmente desciende hasta la ejecución y conserva trazabilidad en el terreno.

## 84. 8 Operación

La cláusula de operación introduce el momento en que el SGIA deja de ser, ante todo, una construcción diseñada para convertirse en una estructura efectivamente activa dentro de la organización. Aquí el sistema tiene que demostrar que sus procesos existen en la práctica, que sus controles están integrados en el funcionamiento cotidiano y que las decisiones tomadas durante la planificación se han traducido en acciones operativas concretas.

Esta cláusula merece una lectura amplia. Operar un SGIA no equivale únicamente a poner controles en marcha. Significa coordinar procesos, supervisar resultados, reaccionar ante cambios, verificar la ejecución y mantener alineación entre lo que fue planificado y lo que

finalmente ocurre. En clave de gestión, la operación es el lugar donde el sistema crea o pierde credibilidad. En clave de gobernanza, es la evidencia más clara de si el liderazgo y la planificación realmente gobiernan la IA o si quedan limitados a un plano declarativo.

## 85. 8.1 Planificación y control operacional

La organización planifica, implementa y controla los procesos necesarios para cumplir los requisitos del SGIA y para implementar las acciones determinadas en la cláusula 6, mediante el establecimiento de criterios para los procesos y la implementación del control de los procesos de acuerdo con esos criterios.

Este requisito establece una idea central: la operación del SGIA no puede dejarse al criterio informal de cada área, ni a la buena voluntad de los equipos, ni a prácticas improvisadas. La organización necesita definir de antemano cómo deben funcionar los procesos relevantes, qué criterios aplican, cómo se verificará su ejecución y qué condiciones deben cumplirse para considerar que operan de forma aceptable.

En la práctica, esto significa traducir las decisiones de planificación en mecanismos de trabajo reales. Si la organización definió controles de riesgo, criterios de impacto, rutas de aprobación, medidas de supervisión o requisitos de documentación, esos elementos deben verse reflejados en la forma en que operan los procesos del sistema. La fortaleza de esta cláusula radica en que exige coherencia entre diseño y ejecución. Un SGIA maduro no funciona por declaraciones generales. Funciona por procesos gobernados.

## 86. 8.1 Planificación y control operacional: implementación de controles relacionados con la operación

La organización implementa los controles determinados de acuerdo con 6.1.3 que estén relacionados con la operación del SGIA, por ejemplo, controles vinculados con el ciclo de vida de desarrollo y uso del sistema de IA.

Aquí la norma conecta directamente la gestión del riesgo con la práctica operativa. Los controles seleccionados durante el tratamiento del riesgo deben migrar desde el plano de la decisión al plano de la acción. Esto implica insertarlos en actividades, secuencias de trabajo, puntos de verificación, responsabilidades de supervisión y flujos documentales. Los controles dejan de existir como una decisión analítica y pasan a formar parte del modo en que la organización opera la IA.

Este punto cobra especial importancia porque una buena parte de los fallos organizacionales en materia de IA no proviene de ausencia total de análisis, sino de una mala transición entre análisis y ejecución. Se identifican riesgos, se seleccionan medidas, pero esas medidas no terminan incorporadas de forma consistente al trabajo cotidiano. ISO/IEC 42001 busca cerrar precisamente esa brecha.

## 87. 8.1 Planificación y control operacional: monitoreo de la eficacia de los controles

La eficacia de los controles implementados debe ser monitoreada y, cuando no se logren los resultados previstos, deben considerarse acciones correctivas. La norma recuerda que el Anexo A enumera controles de referencia y que el Anexo B proporciona orientación para su implementación.

Esta disposición impide que la organización confunda instalación con eficacia. Un control puede existir formalmente y aun así no funcionar como se espera. Puede aplicarse de manera incompleta, quedar desactualizado, ser insuficiente frente a un cambio del entorno o producir una falsa sensación de seguridad. Por ello, el SGIA exige observar si los controles realmente cumplen el propósito para el cual fueron diseñados.

En clave de aseguramiento, este requisito fortalece la disciplina del sistema. No se trata solo de comprobar que el control se ejecutó, sino de revisar si produjo el resultado previsto. Cuando no lo hace, el SGIA debe ser capaz de reaccionar. Ese circuito de observación y ajuste es una de las señales más claras de madurez operativa.

## 88. 8.1 Planificación y control operacional: evidencia de ejecución según lo planificado

La información documentada debe estar disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado. Esta exigencia reafirma el papel de la documentación como soporte de confiabilidad operativa.

La organización necesita conservar evidencia suficiente para demostrar que los procesos no solo estaban definidos, sino que efectivamente se ejecutaron conforme a criterios establecidos. Esa información puede adoptar distintas formas según el contexto: registros de aprobación, evidencias de verificación, bitácoras de monitoreo, resultados de pruebas, trazas de revisión, actas, reportes o cualquier otro artefacto documental que permita reconstruir la ejecución del sistema.

En clave de gestión, esta evidencia cumple varias funciones. Permite sostener confianza, facilita análisis posteriores, mejora la rendición de cuentas y alimenta la evaluación del desempeño. En ausencia de esta trazabilidad, el SGIA pierde capacidad de demostrar consistencia entre lo que dice hacer y lo que realmente hace.

## 89. 8.1 Planificación y control operacional: control de cambios planificados y revisión de cambios no intencionados

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

Este requisito reconoce que la operación del SGIA ocurre en un entorno cambiante. Algunos cambios son deliberados: nuevas versiones de modelos, actualizaciones de datos, ajustes de procesos, modificaciones de alcance, incorporación de nuevos proveedores o cambios regulatorios. Otros cambios pueden producirse sin intención explícita: variaciones inesperadas del comportamiento del sistema, alteraciones indirectas por dependencia de terceros, cambios en el entorno de uso o desviaciones operativas no previstas.

La norma exige que la organización no trate estos cambios como simples incidentes aislados. Debe gobernarlos. Esto implica anticipar consecuencias cuando el cambio es planificado y revisar impactos cuando el cambio emerge de manera no intencionada. En clave senior, esta cláusula protege la estabilidad del sistema y evita que la evolución operativa debilite la coherencia del SGIA.

## 90. 8.1 Planificación y control operacional: control de procesos, productos o servicios proporcionados externamente

La organización asegura que los procesos, productos o servicios proporcionados externamente que sean relevantes para el SGIA estén controlados. Este requisito amplía la lógica del control operacional hacia la dependencia con terceros.

En contextos reales, muchas organizaciones no desarrollan ni operan toda su IA internamente. Utilizan proveedores de tecnología, plataformas, modelos externos, servicios de datos, componentes especializados o consultoría técnica. La norma exige que esa externalización no se convierta en una zona ciega de responsabilidad.

Controlar elementos externos significa reconocer que la organización sigue siendo responsable por la coherencia de su SGIA aunque intervengan terceros. Esto puede requerir cláusulas contractuales, criterios de evaluación, mecanismos de supervisión, documentación de dependencia, validación de entregables o revisión de desempeño. En clave de gobernanza, este requisito protege frente al error de creer que el riesgo desaparece cuando una actividad es subcontratada.

## 91. 8.2 Evaluación de riesgos de IA

La organización realiza evaluaciones de riesgos de IA de acuerdo con lo establecido en 6.1.2, en intervalos planificados o cuando se propongan o ocurran cambios significativos. Esta cláusula traslada el análisis de riesgos desde la fase de planificación hacia la operación viva del sistema.

La norma deja claro que el riesgo no se evalúa una sola vez. Debe revisarse periódicamente y cada vez que el contexto operativo cambie de forma relevante. Esto responde a la naturaleza misma de la IA. Los sistemas pueden evolucionar, sus datos pueden variar, sus casos de uso pueden ampliarse y su entorno regulatorio o social puede modificarse. Por ello, una evaluación antigua puede dejar de ser suficiente.

En términos de implementación, este requisito exige una disciplina de revisión recurrente. En clave de gobernanza, demuestra que la organización no gobierna con información congelada. Reconsidera su exposición al riesgo a medida que la realidad cambia.

## 92. 8.2 Evaluación de riesgos de IA: conservación de resultados

La organización conserva información documentada de los resultados de todas las evaluaciones de riesgos de IA. Este requisito aporta continuidad y capacidad de análisis histórico.

Gracias a esta documentación, la organización puede comparar evaluaciones, detectar tendencias, justificar decisiones y explicar por qué ajustó determinados controles o prioridades. En un SGIA maduro, la gestión del riesgo no depende de recuerdos ni de interpretaciones informales. Se apoya en registros verificables que alimentan la memoria del sistema.

## 93. 8.3 Tratamiento de riesgos de IA

La organización implementa el plan de tratamiento de riesgos de IA de acuerdo con 6.1.3 y verifica su eficacia. Esta cláusula reafirma que el tratamiento del riesgo no concluye con la aprobación del plan. Comienza verdaderamente cuando las medidas seleccionadas se ejecutan.

Implementar el plan significa poner en marcha controles, activar responsables, ajustar procesos, establecer seguimientos y sostener medidas en operación real. Verificar la eficacia, por su parte, implica observar si esas medidas logran reducir o manejar el riesgo según lo esperado. Este segundo componente es fundamental. Un plan sin verificación puede generar la ilusión de control sin aportar seguridad real.

## 94. 8.3 Tratamiento de riesgos de IA: tratamiento de nuevos riesgos identificados

Cuando las evaluaciones de riesgos identifican nuevos riesgos que requieren tratamiento, la organización realiza un proceso de tratamiento de riesgos de acuerdo con 6.1.3 para esos riesgos. Este requisito refuerza la naturaleza adaptativa del SGIA.

La organización no puede limitarse a los riesgos inicialmente contemplados. Debe estar preparada para incorporar nuevas exposiciones, nuevas dependencias y nuevas consecuencias. Un SGIA robusto no es el que presume haber previsto todo. Es el que cuenta con disciplina suficiente para responder cuando aparece algo no previsto.

## 95. 8.3 Tratamiento de riesgos de IA: revisión de opciones ineficaces y actualización del plan

Cuando las opciones de tratamiento definidas por el plan no son eficaces, esas opciones se revisan y validan nuevamente siguiendo el proceso de tratamiento de riesgos de acuerdo con 6.1.3, y el plan de tratamiento se actualiza.

Esta cláusula incorpora una lógica explícita de aprendizaje dentro de la operación. La norma reconoce que no todas las decisiones iniciales serán acertadas o suficientes una vez llevadas al entorno real. Cuando eso ocurra, la organización debe revisar, revalidar y actualizar. El sistema no se protege negando la ineficacia. Se protege corrigiéndola con método.

## 96. 8.3 Tratamiento de riesgos de IA: conservación de resultados del tratamiento

La organización conserva información documentada de los resultados de todos los tratamientos de riesgos de IA. Esta documentación deja trazabilidad sobre qué medidas se aplicaron, cómo se evaluó su eficacia, qué ajustes resultaron necesarios y qué decisiones se tomaron frente al riesgo residual.

En clave de gestión, este histórico favorece aprendizaje entre áreas, fortalece la revisión por la dirección y mejora la calidad de las futuras decisiones de tratamiento.

## 97. 8.4 Evaluación de impacto del sistema de IA

La organización realiza evaluaciones de impacto del sistema de IA de acuerdo con 6.1.4, en intervalos planificados o cuando se propongan cambios significativos. Esta cláusula extiende al plano operativo la misma lógica dinámica que la norma ya exige para el riesgo.

El impacto no puede analizarse una sola vez y darse por cerrado. A medida que cambian los sistemas, los usos, los entornos y las relaciones con partes interesadas, también pueden cambiar las consecuencias sobre personas, grupos y sociedad. La organización necesita, por tanto, revisar periódicamente si la lectura de impacto sigue siendo válida.

## 98. 8.4 Evaluación de impacto del sistema de IA: conservación de resultados

La organización conserva información documentada de los resultados de todas las evaluaciones de impacto del sistema de IA. Esta documentación fortalece trazabilidad, transparencia interna y capacidad de revisión.

En clave de gobernanza, disponer de un histórico de evaluaciones de impacto ayuda a la dirección a comprender no solo el desempeño técnico del sistema, sino también la evolución de sus efectos potenciales y la solidez con la que la organización está gobernando esas consecuencias.

## Cierre del módulo 7

Al concluir este módulo, el participante debe haber comprendido que la operación del SGIA no consiste en ejecutar acciones aisladas. Consiste en sostener procesos controlados, implementar decisiones de tratamiento, monitorear eficacia, gobernar cambios, supervisar dependencias externas y revisar de manera periódica riesgos e impactos.

En la progresión del documento, este módulo demuestra si la arquitectura del sistema entra realmente en funcionamiento. El siguiente módulo toma esa realidad operativa y la convierte en información, juicio y decisión mediante la evaluación del desempeño.

En síntesis, este módulo confirma si el SGIA es realmente un sistema en funcionamiento. Allí donde contexto, liderazgo, planificación y soporte prepararon la arquitectura, la operación demuestra si esa arquitectura produce control real, aprendizaje operativo y capacidad de respuesta sostenida.

# Módulo 8. Evaluación del desempeño

## Introducción al módulo

Una vez que el sistema opera, la norma exige una nueva capacidad: convertir ejecución en visibilidad. Este módulo ocupa ese lugar dentro de la macroestructura. Reúne seguimiento, revisión interna y revisión por la dirección para transformar experiencia operativa en información gobernable.

Un sistema de gestión solo puede gobernarse de forma madura cuando es observado, medido, revisado y discutido con base en información suficiente. Esa es la lógica que articula la cláusula 9 de ISO/IEC 42001. Después de diseñar y operar el SGIA, la organización necesita evaluar si el sistema está produciendo los resultados previstos, si sus controles funcionan, si sus brechas son conocidas y si la alta dirección cuenta con los insumos necesarios para decidir.

Este módulo tiene un valor particular porque transforma el SGIA en una capacidad gobernable. La evaluación del desempeño no se limita a producir indicadores. Crea visibilidad institucional. Permite observar tendencias, validar fortalezas, detectar debilidades, revisar la eficacia del sistema y conectar la información operativa con la dirección ejecutiva.

En un programa de certificación, este bloque debe estudiarse con atención porque articula tres dimensiones complementarias: seguimiento técnico y organizacional, revisión interna estructurada del sistema y revisión por la dirección. Juntas, estas tres dimensiones convierten el desempeño en materia de análisis, juicio y decisión.

## 99. 9 Evaluación del desempeño

La cláusula 9 introduce la necesidad de que el SGIA no solo opere, sino que también sea medido, analizado y revisado. Esta exigencia impide que la organización confunda actividad con eficacia. Un sistema puede estar funcionando de manera intensa y, aun así, no estar logrando sus resultados previstos. Puede producir mucha documentación, muchas reuniones o muchos controles, sin que ello se traduzca en una gestión realmente útil de la IA.

La evaluación del desempeño corrige ese riesgo. Obliga a la organización a observar qué está ocurriendo y a generar una lectura estructurada de esa realidad. En la práctica, esto significa decidir qué conviene medir, cómo se medirá, qué resultados serán analizados y qué conclusiones se derivarán para la mejora o para la toma de decisiones directivas.

En clave AIGPC™, esta cláusula resulta particularmente poderosa porque conecta resultados del sistema con responsabilidad de gobierno. Una dirección que no recibe

información relevante sobre desempeño difícilmente podrá gobernar la IA con criterio. La evaluación del desempeño es, por tanto, una condición previa para la supervisión ejecutiva efectiva.

## 100. 9.1 Monitoreo, medición, análisis y evaluación

La organización determina qué necesita ser monitoreado y medido, así como los métodos para el monitoreo, la medición, el análisis y la evaluación, según corresponda, para asegurar resultados válidos.

Este requisito establece el punto de partida de todo el bloque de evaluación. La organización no debe medir por inercia ni por acumulación de datos. Debe definir de forma deliberada qué información le permitirá comprender el estado del SGIA y cómo obtendrá esa información con la calidad suficiente. Aquí la palabra clave es validez. Los resultados del monitoreo y la medición solo aportan valor si son confiables, relevantes y utilizables para la toma de decisiones.

En el contexto del SGIA, esto puede implicar indicadores sobre cumplimiento de objetivos de IA, eficacia de controles, tratamiento de riesgos, desempeño de procesos, tiempos de respuesta, incidentes, calidad documental, ejecución de revisiones, resultados de planes de remediación u otras métricas pertinentes. Lo importante no es la cantidad, sino la capacidad de cada dato para iluminar el comportamiento del sistema.

## 101. 9.1 Monitoreo, medición, análisis y evaluación: temporalidad del seguimiento

La organización determina cuándo se deben realizar el monitoreo y la medición, y cuándo los resultados de esas actividades deben ser analizados y evaluados. Esta cláusula completa la arquitectura del seguimiento al introducir la dimensión temporal.

La eficacia del SGIA no puede depender de observaciones esporádicas o improvisadas. La organización necesita una cadencia. Debe saber con qué frecuencia monitorea, cuándo mide, cuándo analiza y en qué momento convierte esa información en evaluación útil. Esta temporalidad debe ser coherente con el nivel de riesgo, la criticidad de los procesos, la naturaleza de los sistemas de IA y la dinámica del entorno.

En clave de madurez, la existencia de esta cadencia es un signo importante. Muestra que la organización no espera a tener problemas visibles para mirar el sistema. Mantiene una disciplina periódica de observación.

## 102. 9.1 Monitoreo, medición, análisis y evaluación: evidencia documentada

La información documentada debe estar disponible como evidencia de los resultados del monitoreo, la medición, el análisis y la evaluación. Esta exigencia protege la trazabilidad del juicio organizacional sobre el sistema.

No basta con afirmar que se revisó el desempeño. La organización debe conservar evidencia de qué observó, qué midió, qué interpretó y qué conclusiones extrajo. Esa documentación fortalece la rendición de cuentas, facilita revisiones posteriores y sirve de insumo para la dirección, para la mejora y para procesos de certificación.

## 103. 9.1 Monitoreo, medición, análisis y evaluación: desempeño y eficacia del SGIA

La organización evalúa el desempeño y la eficacia del SGIA. Esta frase resume el propósito del bloque. Monitorear y medir no es un fin en sí mismo. El fin es entender si el sistema está funcionando y si realmente produce los efectos previstos.

La distinción entre desempeño y eficacia también merece atención. El desempeño permite observar resultados y tendencias. La eficacia permite emitir un juicio sobre si el sistema, tal como está diseñado y operado, es suficiente para alcanzar sus objetivos. Esa combinación transforma información en criterio de gestión.

## 104. 9.2 Revisión interna del sistema

La cláusula 9.2 introduce la revisión interna del sistema como parte del SGIA. En esta versión de autoestudio se presenta como un proceso estructurado de aseguramiento interno que ayuda a revisar la coherencia, la implementación y el mantenimiento del sistema desde dentro de la organización.

Aunque el lenguaje técnico de la norma conserva el término auditoría interna, aquí interesa sobre todo su función. La revisión interna del sistema no se orienta solo a detectar incumplimientos. Produce información ordenada sobre el estado del SGIA, identifica brechas, valida prácticas sólidas y alimenta la mejora continua. En esencia, actúa como un mecanismo de aprendizaje institucional con disciplina metodológica.

## 105. 9.2.1 General

La organización realiza revisiones internas a intervalos planificados para proporcionar información sobre si el SGIA cumple con los requisitos propios de la organización para su sistema de gestión de IA y con los requisitos de ISO/IEC 42001.

Esta disposición establece la función básica del aseguramiento interno: contrastar la realidad del sistema frente a referentes definidos. La revisión no se hace sobre percepciones vagas. Se realiza respecto de criterios concretos: requisitos internos y

requisitos de la norma. De ese contraste surge información valiosa para comprender si el SGIA está alineado con lo que afirma ser.

En clave de gestión, esta cláusula fortalece la integridad del sistema. La organización deja de depender exclusivamente de autoevaluaciones informales y dispone de un mecanismo periódico para revisar coherencia y consistencia.

## 106. 9.2.1 General: implementación y mantenimiento eficaz del sistema

La organización asegura también que el SGIA esté implementado y mantenido eficazmente. Esta segunda parte de 9.2.1 es especialmente importante porque amplía el foco más allá de la conformidad formal.

Un sistema puede cumplir en apariencia con determinados requisitos documentales y, aun así, no estar funcionando con eficacia. Por ello, la revisión interna debe observar no solo si existe documentación o estructura, sino además si los procesos operan, si los controles se sostienen, si las responsabilidades están activas y si el sistema sigue siendo útil en el contexto real de la organización.

## 107. 9.2.2 Programa de revisión interna

La organización planifica, establece, implementa y mantiene uno o más programas de revisión interna que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Este requisito convierte la revisión interna en una práctica organizada y no ocasional. La organización necesita una estructura metodológica para revisar su SGIA a lo largo del tiempo. Esa estructura debe definir cómo se programarán las revisiones, con qué alcance, con qué métodos, bajo qué responsabilidades y con qué productos de salida.

En clave de madurez, contar con un programa de revisión interna significa haber institucionalizado el aprendizaje y el aseguramiento del sistema. Ya no depende de iniciativas aisladas. Pasa a formar parte de la lógica regular del SGIA.

## 108. 9.2.2 Programa de revisión interna: importancia de procesos y resultados de revisiones previas

Al establecer el programa de revisión interna, la organización considera la importancia de los procesos involucrados y los resultados de revisiones previas. Este criterio introduce una lógica de priorización.

No todos los procesos tienen el mismo peso para el logro de resultados ni todos presentan el mismo nivel de criticidad o exposición. Tampoco todas las áreas evolucionan de la

misma forma. Al considerar la relevancia de los procesos y el historial de resultados anteriores, la organización puede orientar mejor sus esfuerzos de revisión hacia donde más valor aportan.

## 109. 9.2.2 Programa de revisión interna: objetivos, criterios, alcance, objetividad e imparcialidad

La organización define los objetivos, criterios y alcance de cada revisión, y selecciona a quienes la realizan de manera que se aseguren objetividad e imparcialidad. Este requisito protege la credibilidad del proceso.

Cada revisión necesita una finalidad clara, un referente preciso y un perímetro delimitado. Además, debe ser conducida por personas capaces de sostener juicio técnico sin conflictos que comprometan la objetividad. En la práctica, esto no siempre es sencillo, especialmente en organizaciones pequeñas. Pero la norma exige que se hagan esfuerzos razonables para proteger la independencia funcional del proceso de revisión.

## 110. 9.2.2 Programa de revisión interna: información a responsables pertinentes

La organización asegura que los resultados de las revisiones internas se informen a los responsables pertinentes. Este requisito conecta el aseguramiento con la acción.

Una revisión solo genera valor real cuando sus resultados llegan a quienes pueden decidir, corregir, reforzar o escalar acciones. Informar resultados no es un mero cierre administrativo. Es el paso que activa accountability y permite que el SGIA aprenda de su propia observación estructurada.

## 111. 9.2.2 Programa de revisión interna: evidencia del programa y de los resultados

La información documentada debe estar disponible como evidencia de la implementación del programa de revisión interna y de los resultados de las revisiones. Esta documentación fortalece la trazabilidad del aseguramiento y demuestra que la organización no solo planifica revisiones, sino que efectivamente las realiza y utiliza sus resultados.

## 112. 9.3 Revisión por la dirección

La cláusula 9.3 introduce la revisión por la dirección como uno de los mecanismos más importantes de gobierno dentro del SGIA. A través de esta revisión, la alta dirección no solo recibe información. Evalúa de forma estructurada si el sistema sigue siendo adecuado, útil y eficaz.

En clave de gobernanza, este es el espacio donde el desempeño del SGIA se convierte en decisión ejecutiva. Los resultados de monitoreo, revisiones internas, cambios del contexto y oportunidades de mejora dejan de ser simples insumos técnicos y pasan a formar parte de la agenda directiva.

## 113. 9.3.1 General

La alta dirección revisa el SGIA a intervalos planificados para asegurar su conveniencia, adecuación y eficacia continuas. Esta cláusula obliga a la dirección a mantener una relación activa con el sistema.

La revisión por la dirección no se limita a verificar si el SGIA existe. Se orienta a confirmar si sigue siendo pertinente para el contexto, si mantiene utilidad práctica y si continúa produciendo los resultados esperados. En otras palabras, la dirección debe ejercer un juicio de vigencia sobre el sistema.

## 114. 9.3.2 Entradas de la revisión por la dirección: acciones previas y cambios del contexto

La revisión por la dirección incluye el estado de las acciones de revisiones anteriores y los cambios en cuestiones externas e internas que sean relevantes para el SGIA. Este requisito aporta continuidad histórica y sensibilidad al entorno.

La alta dirección necesita saber qué decisiones previas se implementaron, cuáles siguen abiertas y cómo ha cambiado el contexto desde la última revisión. Sin esta memoria, la revisión pierde profundidad y puede convertirse en un ejercicio desconectado de la evolución real del sistema.

## 115. 9.3.2 Entradas de la revisión por la dirección: partes interesadas y tendencias en desviaciones del estándar

La revisión por la dirección incluye también cambios en las necesidades y expectativas de las partes interesadas relevantes, así como información sobre el desempeño del SGIA, incluidas las tendencias en desviaciones del estándar y acciones de remediación.

Esta entrada es especialmente importante porque amplía la mirada ejecutiva más allá del dato interno. La dirección necesita entender si el entorno de expectativas cambió y si el sistema muestra patrones de desviación que merecen atención. La noción de tendencia es muy valiosa aquí. Una desviación aislada puede requerir corrección. Una tendencia puede exigir decisión estructural.

## 116. 9.3.2 Entradas de la revisión por la dirección: resultados de seguimiento, revisiones internas y oportunidades de mejora

La revisión por la dirección incluye además los resultados del monitoreo y la medición, los resultados de las revisiones internas y las oportunidades de mejora continua. Esta disposición convierte la revisión por la dirección en un punto de convergencia del SGIA.

En ese espacio se reúnen indicadores, hallazgos, señales de alerta y posibilidades de fortalecimiento. Cuando estos elementos se analizan en conjunto, la dirección puede emitir un juicio más completo sobre el estado del sistema y sobre las decisiones que conviene adoptar.

## 117. 9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección incluyen decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambios en el SGIA. Esta cláusula deja claro que la revisión no es meramente informativa. Debe producir decisiones.

La dirección necesita traducir el análisis de entradas en acciones concretas: mantener el rumbo, priorizar ajustes, reforzar controles, redefinir responsabilidades, revisar recursos o introducir modificaciones estructurales en el sistema. Así, la revisión por la dirección se convierte en un mecanismo real de gobierno.

## 118. 9.3.3 Resultados de la revisión por la dirección: evidencia documentada

La información documentada debe estar disponible como evidencia de los resultados de las revisiones por la dirección. Esta trazabilidad protege accountability y continuidad directiva.

La organización necesita conservar registro de qué analizó la dirección, qué decisiones tomó y cómo esas decisiones se conectan con la evolución posterior del SGIA. Esa evidencia resulta esencial para seguimiento, mejora y certificación.

## Cierre del módulo 8

Al finalizar este módulo, el participante debe haber comprendido que la evaluación del desempeño no es una capa adicional del SGIA, sino una de sus funciones esenciales. Gracias a ella, la organización observa el sistema, revisa su coherencia, obtiene información estructurada desde dentro y la convierte en materia de decisión directiva.

En la secuencia del documento, este módulo prepara el terreno para la mejora. Una vez que el sistema ha sido observado, medido y revisado, la organización debe ser capaz de corregir, fortalecer y evolucionar lo aprendido.

En síntesis, este módulo demuestra cómo el SGIA se vuelve gobernable: mediante monitoreo, medición, revisión interna y revisión por la dirección. Sin estas capacidades, el sistema podría existir, pero no aprendería de sí mismo ni ofrecería a la dirección la visibilidad necesaria para conducir la IA con autoridad y criterio.

# Módulo 9. Mejora

## Introducción al módulo

Este módulo cierra el ciclo central del SGIA. Después de operar y evaluar, la organización debe demostrar que puede transformar hallazgos y desviaciones en fortalecimiento real del sistema.

Todo sistema de gestión maduro necesita una capacidad explícita de evolución. ISO/IEC 42001 recoge esta exigencia en la cláusula 10. Después de comprender el contexto, establecer liderazgo, planificar riesgos y objetivos, habilitar soporte, operar procesos y evaluar desempeño, la organización debe ser capaz de fortalecer el SGIA de manera continua y de responder con disciplina cuando aparece una desviación del estándar.

La mejora, en este marco, no se limita a corregir errores. Expresa una filosofía de madurez. Una organización que gestiona IA de manera responsable sabe que el sistema nunca queda terminado de forma definitiva. Cambian los riesgos, cambian las expectativas, cambian los usos y cambian las condiciones del entorno. Por ello, el SGIA necesita aprender, ajustarse y refinarse de manera recurrente.

Desde el punto de vista del autoestudio, este módulo debe entenderse como el cierre lógico del ciclo PHVA. No basta con planificar, hacer y verificar. Además hay que actuar sobre lo aprendido. Esa capacidad de reacción y fortalecimiento es la que convierte al SGIA en una estructura viva, no en un mecanismo estático de control.

## 119. 10 Mejora

La cláusula 10 reúne el componente de evolución explícita del SGIA. Después de revisar desempeño, riesgos, impactos, revisiones internas y decisiones de dirección, la organización necesita una lógica clara para fortalecer el sistema y responder a sus debilidades o limitaciones.

Esta cláusula cumple una función integradora. Todo lo que el SGIA aprende en sus etapas anteriores debe poder traducirse en ajustes reales. Si el sistema detecta desviaciones y no cambia, su capacidad de gestión se debilita. Si genera información pero no la convierte en fortalecimiento, la mejora continua queda vacía. Por eso, ISO/IEC 42001 ubica la mejora como una fase específica del sistema, pero al mismo tiempo la proyecta como una capacidad transversal.

## 120. 10.1 Mejora continua

La organización mejora continuamente la idoneidad, adecuación y eficacia del SGIA. Este requisito resume uno de los principios más importantes de la norma.

Mejorar continuamente significa revisar si el sistema sigue siendo pertinente para el contexto, suficiente para los riesgos e impactos que enfrenta y eficaz para lograr los resultados previstos. La mejora continua no se limita a resolver fallas puntuales. Además incluye fortalecer capacidades, refinar procesos, optimizar controles, enriquecer documentación, desarrollar competencias y elevar la madurez general del sistema.

En clave aplicada, esta cláusula convierte al SGIA en una estructura que aprende. Cada revisión, cada indicador, cada evaluación de riesgo, cada resultado de impacto y cada decisión de la dirección pueden convertirse en insumos para robustecer el sistema. Ese aprendizaje acumulativo es uno de los mayores valores de un sistema de gestión bien implementado.

## 121. 10.2 Desviación del estándar y plan de remediación

Cuando ocurre una desviación del estándar, la organización reacciona a ella y, según corresponda, toma acciones para controlarla y corregirla, así como para tratar sus consecuencias. Esta cláusula marca el paso desde la detección del problema hacia la respuesta estructurada.

La organización no puede limitarse a registrar la desviación. Debe actuar. Controlar significa contener el efecto inmediato. Corregir significa resolver la situación observada. Tratar consecuencias significa reconocer que una desviación puede haber generado efectos sobre procesos, controles, personas, resultados o confianza. El SGIA exige una respuesta completa, no un simple cierre administrativo.

## 122. 10.2 Desviación del estándar y plan de remediación: análisis de causas

La organización evalúa la necesidad de acciones para eliminar la causa o causas de la desviación del estándar, con el fin de que no vuelva a ocurrir o no ocurra en otra parte, mediante la revisión de la desviación y la determinación de sus causas.

Aquí la norma introduce una dimensión esencial de la mejora: el análisis causal. Corregir el síntoma no basta. La organización necesita comprender por qué apareció la desviación y qué condiciones del sistema permitieron que se produjera. Esa comprensión es la base de una remediación durable.

En clave de madurez, esta cláusula protege frente a soluciones superficiales. El SGIA no se fortalece solo apagando incendios. Se fortalece cuando utiliza cada desviación como oportunidad para revisar procesos, criterios, competencias, controles o mecanismos de coordinación.

## 123. 10.2 Desviación del estándar y plan de remediación: alcance sistémico y revisión de eficacia

La organización determina si existen desviaciones similares o si potencialmente podrían ocurrir, implementa cualquier acción necesaria y revisa la eficacia de cualquier acción tomada. Esta parte del requisito amplía la mejora más allá del caso puntual.

La norma invita a una mirada sistémica. Una desviación observada en un punto puede ser señal de una debilidad más amplia. La organización necesita preguntarse si otras áreas, procesos o sistemas comparten condiciones similares. Además, debe verificar si la remediación implementada realmente resolvió el problema. De este modo, la mejora deja de ser local y se convierte en una práctica de fortalecimiento transversal.

## 124. 10.2 Desviación del estándar y plan de remediación: cambios en el SGIA

La organización realiza cambios en el SGIA cuando sea necesario. Esta cláusula deja claro que la mejora puede requerir modificaciones reales del sistema.

No todas las desviaciones se resuelven con una instrucción puntual o con una corrección menor. Algunas obligan a rediseñar procesos, revisar controles, ajustar roles, modificar documentación, reforzar recursos o replantear mecanismos de seguimiento. El SGIA debe tener la flexibilidad y la disciplina necesarias para introducir esos cambios cuando la situación lo exige.

## 125. 10.2 Desviación del estándar y plan de remediación: proporcionalidad de la remediación

Las acciones de remediación son apropiadas a los efectos de las desviaciones del estándar encontradas. Este criterio introduce una exigencia de proporcionalidad.

No todas las desviaciones tienen la misma magnitud, criticidad o capacidad de afectar los resultados del sistema. Por ello, la remediación debe guardar correspondencia con el impacto real de la brecha observada. La organización necesita evitar tanto la respuesta insuficiente como la sobrerreacción. La mejora eficaz es aquella que ajusta con criterio.

## 126. 10.2 Desviación del estándar y plan de remediación: evidencia documentada

La información documentada debe estar disponible como evidencia de la naturaleza de las desviaciones del estándar y de cualquier acción posterior tomada, así como de los resultados de cualquier acción de remediación. Esta exigencia cierra el ciclo de mejora con trazabilidad.

La organización necesita conservar evidencia de qué ocurrió, cómo interpretó la desviación, qué acciones implementó y qué resultados produjo la remediación. Esa memoria fortalece continuidad, aprendizaje y capacidad de revisión futura. Además permite que la dirección y otras funciones relevantes comprendan si el sistema está corrigiendo sus brechas con eficacia.

## Cierre del módulo 9

Al concluir este módulo, el participante debe comprender que la mejora en ISO/IEC 42001 no es un complemento opcional del SGIA. Es una capacidad estructural. Gracias a ella, la organización fortalece la idoneidad, adecuación y eficacia del sistema, y responde de manera disciplinada cuando detecta desviaciones del estándar.

Con este módulo concluye la tercera parte del documento: la dedicada a ejecución, revisión y mejora. A continuación comienza una cuarta parte orientada a la arquitectura de apoyo del sistema, los anexos de implementación y el aseguramiento interno ampliado.

En síntesis, este módulo cierra el ciclo del sistema con una idea poderosa: la gestión responsable de la IA no se demuestra por ausencia total de problemas, sino por la capacidad institucional de aprender, corregir y evolucionar con rigor cada vez que el sistema lo necesita.

# Módulo 10. Anexo A: Controles de referencia

## Introducción al módulo

La cuarta parte del documento amplía y consolida lo ya estudiado. Su función es mostrar cómo las cláusulas principales se apoyan en controles de referencia, guías de implementación, criterios de adaptación sectorial, metodologías de aseguramiento y una síntesis final del sistema.

Después de recorrer las cláusulas principales del SGIA, la norma presenta en el Anexo A una arquitectura de controles de referencia que ayuda a traducir los requisitos del sistema en medidas más concretas de gestión y control. En este material de autoestudio, el Anexo A no debe tratarse como un apéndice secundario ni como una simple lista complementaria. Debe estudiarse como uno de los grandes puentes entre el diseño normativo del SGIA y su implementación efectiva.

Las cláusulas 4 a 10 establecen qué exige la norma en materia de contexto, liderazgo, planificación, soporte, operación, evaluación y mejora. El Anexo A ayuda a responder otra pregunta igual de importante: qué clase de controles conviene considerar para sostener esos requisitos en la práctica. Esa es la razón por la cual su papel dentro del programa de certificación resulta tan relevante. Permite al participante pasar del entendimiento general del sistema a una lectura más concreta de su arquitectura de control.

En clave AIMPC™, el Anexo A resulta especialmente útil porque orienta decisiones de implementación y permite estructurar respuestas operativas con mayor precisión. En clave AIGPC™, su valor también es alto, ya que muestra cómo la gobernanza de la IA se materializa en mecanismos específicos de dirección, supervisión, trazabilidad y relación con partes interesadas. Dicho de otro modo, el Anexo A convierte la ambición del SGIA en una gramática de control.

## 127. Anexo A: Controles

El Anexo A presenta los controles de referencia que apoyan la implementación del SGIA. Debe entenderse como una estructura de apoyo para que la organización traduzca riesgos, objetivos y decisiones de gobernanza en medidas operativas y organizacionales más visibles. No sustituye el análisis de riesgos ni el juicio institucional. Tampoco agota por completo las necesidades de control de cada entorno. Su función es ofrecer una base estructurada y reconocible sobre la cual construir o contrastar la arquitectura de control del sistema.

En la práctica, esto significa que la organización puede utilizar el Anexo A para verificar si sus respuestas al riesgo son suficientes, si existen vacíos relevantes o si su marco de

control necesita mayor desarrollo. En clave pedagógica, esta función resulta especialmente valiosa porque ayuda al participante a no quedarse en el nivel abstracto de las cláusulas. El Anexo A muestra cómo se concretan muchas de las exigencias del SGIA en mecanismos más tangibles.

También conviene destacar que el Anexo A dialoga de forma directa con la Declaración de Aplicabilidad. Esto refuerza su relevancia en implementación y certificación. Los controles de referencia no solo orientan. Además permiten justificar decisiones de inclusión, exclusión y complemento, mostrando de manera más clara cómo la organización relaciona riesgo, control y responsabilidad.

## 128. Anexo A: Cláusulas, objetivos y controles

El Anexo A se organiza en nueve grupos y reúne treinta y ocho controles. Entre esos grupos se incluyen políticas relacionadas con IA, organización interna, recursos para sistemas de IA, evaluación de impactos, ciclo de vida del sistema de IA, datos para sistemas de IA, información para partes interesadas, uso de sistemas de IA y relaciones con terceros y clientes.

Esta estructura tiene un enorme valor formativo. Demuestra que la gestión de IA no se reduce a una sola dimensión, ni puede resolverse únicamente mediante controles tecnológicos. La organización necesita combinar dirección institucional, roles claros, recursos, sensibilidad frente a impacto, disciplina sobre el ciclo de vida, control de datos, comunicación adecuada, responsabilidad de uso y supervisión de relaciones externas. El Anexo A, en ese sentido, ofrece una visión integral del SGIA aplicada al terreno de los controles.

En clave de madurez, esta diversidad también transmite una idea importante: la IA es una capacidad transversal. Sus controles atraviesan decisiones estratégicas, procesos operativos, flujos documentales y relaciones con terceros. Quien estudia este anexo con atención comprende mejor por qué ISO/IEC 42001 no puede tratarse como una norma solo técnica.

## 129. Anexo A: Controles sobre políticas, organización interna, recursos e impactos

Dentro de los grupos del Anexo A se incluyen, entre otros, controles relacionados con políticas de IA, como la política misma, su alineación con otras políticas organizacionales y su revisión; controles de organización interna, como roles, responsabilidades y reporte de preocupaciones; controles sobre recursos para sistemas de IA, como documentación de recursos, datos, herramientas, sistemas y recursos humanos; y controles sobre

evaluación de impactos, incluyendo proceso, documentación, evaluación sobre individuos y grupos, e impactos sociales.

Este primer bloque de controles merece una lectura detenida porque deja ver el costado institucional de la arquitectura del SGIA. La norma no entiende la IA solo como un asunto de desarrollo o despliegue tecnológico. La sitúa dentro de una estructura más amplia de dirección, recursos y consideración de efectos. Los controles sobre política confirman que la organización necesita orientación formal. Los controles sobre organización interna evidencian que el sistema requiere accountability y canales de reporte. Los controles sobre recursos recuerdan que la capacidad de gobernar la IA depende de medios concretos. Y los controles sobre impacto introducen una sensibilidad que va más allá del rendimiento técnico.

En términos de implementación, este conjunto ayuda a construir la capa de base del SGIA. Sin políticas claras, sin estructura interna definida, sin recursos suficientes y sin consideración del impacto, la organización puede desplegar IA, pero difícilmente podrá afirmar que la gestiona con madurez.

## 130. Anexo A: Controles sobre ciclo de vida, datos, información, uso y relaciones externas

El Anexo A también incluye controles relacionados con el ciclo de vida del sistema de IA, como gestión para el desarrollo, objetivos para el desarrollo responsable, procesos de diseño y desarrollo, requisitos y especificaciones, documentación técnica, verificación, validación, despliegue, operación, monitoreo y registro de eventos. Además, incorpora controles sobre datos para sistemas de IA, como adquisición, calidad, procedencia y preparación de datos; sobre información para partes interesadas, como documentación del sistema, reporte externo, comunicación de incidentes e información relevante; sobre uso de sistemas de IA; y sobre relaciones con terceros y clientes.

Este segundo bloque amplía la visión del SGIA hacia todo el ecosistema funcional de la IA. Permite comprender que la organización debe tomar decisiones no solo sobre riesgos y política, sino también sobre cómo se diseña, desarrolla, documenta, explica, usa y supervisa la IA a lo largo de su ciclo de vida y en relación con actores externos.

En clave AIMPC™, estos controles ayudan a construir una arquitectura de implementación más robusta. En clave AIGPC™, muestran cómo la responsabilidad institucional se distribuye a través de distintos momentos y dependencias del sistema. Juntos, estos controles convierten al Anexo A en una referencia decisiva para una gestión completa, trazable y defendible.

## Integración conceptual del módulo 10

El Anexo A debe estudiarse como un mapa de la madurez operativa del SGIA. No reemplaza el juicio organizacional ni clausura el análisis de riesgos, pero sí orienta el diseño de la arquitectura de control y ayuda a comprobar si una organización está abordando las dimensiones correctas.

Su mayor virtud pedagógica consiste en hacer visible que la gestión de IA se construye mediante un sistema de controles articulados, no mediante acciones aisladas. La política sin control operativo es insuficiente. El control operativo sin gobierno de datos es frágil. El tratamiento de riesgos sin documentación y sin comunicación a partes relevantes queda incompleto. El Anexo A, justamente, permite ver esas interdependencias.

## Cierre del módulo 10

Al concluir este módulo, el participante debe comprender que el Anexo A no es un agregado periférico de ISO/IEC 42001. Es la referencia central para transformar objetivos y riesgos en controles concretos. Su valor reside en ayudar a la organización a construir una arquitectura de control suficientemente amplia para abarcar dirección, operación, impacto, datos, uso y relaciones externas.

En la secuencia de esta cuarta parte, el Anexo A establece la base de control. El módulo siguiente amplía esa base con guías de implementación, ejemplos de objetivos y riesgos, y claves de adaptación sectorial.

En síntesis, el Anexo A enseña cómo el SGIA se vuelve controlable en términos prácticos. Donde las cláusulas principales indican qué requiere el sistema, los controles de referencia muestran con mayor claridad cómo puede materializarse esa exigencia dentro de la organización.

# Módulo 11. Anexos B, C y D como apoyo para la implementación del SGIA

## Introducción al módulo

Si el módulo anterior consolidó la arquitectura de control, este módulo amplía la capacidad de implementación y adaptación del SGIA. Su papel dentro de la macroestructura es convertir la referencia de control en guía práctica, criterio ampliado y lectura sectorial.

Si el Anexo A ofrece la estructura de controles de referencia, los Anexos B, C y D amplían la capacidad de la organización para interpretar, aterrizar y adaptar el SGIA. En un material de certificación, estos anexos no deben leerse como notas auxiliares de baja prioridad. Cumplen funciones pedagógicas y técnicas de gran valor: ayudan a traducir controles en prácticas de implementación, amplían el criterio para formular objetivos y riesgos, y muestran cómo aplicar el SGIA en distintos sectores y dominios.

El participante debe estudiar este módulo con una idea muy clara: ISO/IEC 42001 no fue diseñada para operar como una norma aislada y rígida. Fue concebida como un sistema suficientemente estructurado para ofrecer consistencia, pero también suficientemente flexible para adaptarse a contextos diversos. Los Anexos B, C y D son una manifestación directa de esa flexibilidad guiada.

## 131. Anexo B: Guía de implementación para controles de IA

El Anexo B proporciona orientación para la implementación de los controles listados en el Anexo A. Su propósito es apoyar a las organizaciones en la aplicación práctica de los controles relacionados con el diseño, desarrollo, provisión o uso de sistemas de IA. Además, sigue la misma estructura de controles definida en el Anexo A.

Esta correspondencia estructural es muy útil desde el punto de vista del estudio. Permite que el participante relacione cada control con una guía de aterrizaje más concreta. En otras palabras, el Anexo A ayuda a decidir qué controles considerar, y el Anexo B ayuda a pensar cómo implementarlos con mayor sentido práctico.

En términos de implementación, esto evita una de las debilidades más frecuentes de los sistemas de gestión: seleccionar controles sin comprender realmente cómo integrarlos al funcionamiento de la organización. El Anexo B no ofrece una receta única, pero sí facilita una interpretación más rica y operativa.

## 132. Anexo B: Relación entre Anexo A y Anexo B

Los controles listados en el Anexo A proporcionan objetivos de control y controles de referencia, mientras que el Anexo B proporciona orientación de implementación para esos controles. Esta relación es clave para entender la lógica aplicada de ISO/IEC 42001.

El Anexo A responde principalmente al qué controlar. El Anexo B ayuda a responder al cómo implementarlo. La organización necesita ambos niveles de lectura. Si se queda solo en el Anexo A, corre el riesgo de adoptar controles sin comprensión suficiente de su propósito operativo. Si se queda solo en el Anexo B sin anclarlo al marco del Anexo A, puede perder consistencia estructural. La combinación de ambos fortalece el diseño y la justificación del SGIA.

En clave de certificación, esta articulación mejora la capacidad del participante para leer la norma con criterio. Ya no se trata de memorizar listas. Se trata de comprender relaciones: riesgo, objetivo de control, control de referencia, enfoque de implementación y evidencia esperada.

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

El Anexo B incluye orientación para políticas relacionadas con IA, organización interna y recursos para sistemas de IA. En B.2, se orienta a establecer, implementar y mantener políticas organizacionales relacionadas con el desarrollo o uso de sistemas de IA. En B.3, se ofrecen lineamientos para definir responsabilidades organizacionales, estructuras de gobernanza y mecanismos para reportar preocupaciones relacionadas con sistemas de IA. En B.4, la orientación se enfoca en identificar, documentar y gestionar los recursos necesarios para el desarrollo, implementación y operación de sistemas de IA.

Estos apartados refuerzan tres pilares del SGIA: dirección, estructura y capacidad. La política da marco. La organización interna distribuye responsabilidades. Los recursos hacen posible la ejecución. Estudiados en conjunto, permiten comprender que la gobernanza de IA necesita tanto voluntad institucional como soporte operativo suficiente.

En clave senior, estos bloques muestran cómo la norma convierte liderazgo en arquitectura. La alta dirección no solo define intención; además habilita una estructura y un entorno de recursos para que el sistema sea sostenible.

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

El Anexo B también ofrece orientación para la evaluación de impactos de sistemas de IA y para el ciclo de vida del sistema de IA. En B.5, se propone apoyo para establecer procesos que permitan evaluar impactos potenciales sobre individuos, grupos y sociedad. En B.6, la orientación ayuda a definir criterios y procesos para las distintas etapas del ciclo de vida

del sistema de IA, incluyendo diseño, desarrollo, verificación, validación, despliegue y operación.

Estos apartados resultan especialmente valiosos porque conectan la gestión del sistema con sus efectos y con su evolución técnica y operativa. La evaluación de impactos obliga a una lectura más amplia del uso de IA. La orientación sobre ciclo de vida, por su parte, permite estructurar controles a lo largo de todo el recorrido del sistema, evitando que la organización concentre su atención solo en el despliegue o solo en el análisis inicial.

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

La guía de implementación aborda también los datos para sistemas de IA y la información para partes interesadas. En B.7, se orienta sobre la gestión de datos utilizados en sistemas de IA, incluyendo adquisición, calidad, procedencia y preparación. En B.8, se ofrece apoyo para proporcionar información adecuada a las partes interesadas relevantes sobre el sistema de IA y sus posibles impactos.

Estos dos apartados ayudan a vincular dos dimensiones esenciales de la confianza en IA: calidad de la base de datos y calidad de la comunicación. Los datos condicionan desempeño, sesgo, robustez y legitimidad del sistema. La información a partes interesadas condiciona transparencia, comprensión y aceptación. Ambos componentes resultan indispensables para una gobernanza seria.

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

El Anexo B incluye además orientación sobre el uso de sistemas de IA y sobre las relaciones con terceros y clientes. En B.9, la orientación se centra en asegurar que los sistemas de IA se utilicen de manera responsable y de acuerdo con las políticas organizacionales. En B.10, se aborda la gestión de responsabilidades, riesgos y obligaciones cuando terceros participan en el ciclo de vida de los sistemas de IA.

Estos apartados recuerdan que el SGIA no termina en el diseño del sistema ni en la documentación técnica. También debe asegurar que el uso real se mantenga dentro de los criterios previstos y que la participación de terceros no genere vacíos de control o de accountability. Aquí se vuelve especialmente visible la dimensión ecosistémica de la IA.

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

El Anexo C proporciona ejemplos de posibles objetivos organizacionales relacionados con sistemas de IA y de fuentes de riesgo relacionadas con IA. La norma aclara que estos ejemplos no son exhaustivos y que pueden variar según el contexto de la organización.

Este anexo cumple una función pedagógica de gran valor. Amplía el criterio. Ayuda a la organización a no pensar sus objetivos o sus riesgos de manera limitada, y ofrece referencias útiles para enriquecer el proceso de planificación. En lugar de imponer listas cerradas, invita a una reflexión más madura sobre para qué utiliza la IA y qué clases de incertidumbre pueden afectar ese propósito.

## 138. Anexo C: Ejemplos de objetivos organizacionales relacionados con IA

Entre los ejemplos de objetivos organizacionales relacionados con sistemas de IA, la norma menciona mejorar la eficiencia o eficacia de procesos organizacionales, apoyar la toma de decisiones basada en datos, mejorar productos o servicios mediante el uso de IA, permitir nuevas capacidades organizacionales y mejorar la experiencia del usuario.

Estos ejemplos muestran que los objetivos de IA pueden vincularse tanto con resultados internos como con valor externo para usuarios, clientes u otros stakeholders. El anexo ayuda a evitar una formulación pobre o excesivamente técnica de objetivos. Además recuerda que los objetivos deben derivar de la estrategia y del propósito organizacional, no de la mera disponibilidad de una herramienta tecnológica.

## 139. Anexo C: Ejemplos de fuentes de riesgo relacionadas con IA

Entre las fuentes de riesgo relacionadas con sistemas de IA, la norma menciona la calidad insuficiente de los datos, la falta de transparencia o explicabilidad, los sesgos en datos o modelos, el uso indebido del sistema y los cambios inesperados en su comportamiento.

Este listado ayuda a ampliar la mirada sobre el riesgo. Muestra que la organización debe considerar tanto problemas técnicos como factores de contexto, calidad de información, comportamiento emergente, opacidad y usos no previstos. En clave de madurez, este anexo funciona como un recordatorio útil: la IA genera riesgos diversos, y el SGIA necesita una visión integral para gestionarlos con criterio.

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

El Anexo D describe cómo el SGIA puede aplicarse en diferentes dominios o sectores. La norma indica que el sistema puede ser utilizado por organizaciones en diversos contextos, incluyendo desarrollo de sistemas de IA, provisión de productos o servicios que utilizan IA y uso de sistemas de IA desarrollados por terceros.

Este punto resulta especialmente relevante porque confirma la amplitud sectorial de ISO/IEC 42001. La norma no está reservada a empresas tecnológicas ni a un único modelo

de uso de IA. Puede adaptarse a distintos tamaños, sectores y posiciones dentro del ecosistema. Esa flexibilidad amplía su valor comercial y formativo.

## 141. Anexo D: Aplicación del sistema de gestión de IA

El SGIA puede aplicarse a lo largo del ciclo de vida de los sistemas de IA. Esto incluye diseño y desarrollo, integración en productos o servicios, operación y monitoreo.

La importancia de este punto reside en que muestra la amplitud temporal del sistema. La gestión de IA no se agota al momento del diseño, ni al desplegar un modelo, ni al hacer seguimiento. Abarca la totalidad del recorrido del sistema. Esta visión ayuda a la organización a ubicar mejor dónde necesita mayor nivel de control, qué evidencias debe conservar y qué actores participan en cada etapa.

## 142. Anexo D: Consideraciones sectoriales

Los requisitos y controles del SGIA pueden aplicarse en diferentes sectores. La organización adapta la implementación según el sector o dominio en que opera, el tipo de sistemas de IA utilizados y los requisitos regulatorios aplicables.

Esta aclaración refuerza uno de los principios más útiles de ISO/IEC 42001: su adaptabilidad. La estructura del sistema es común, pero su profundidad, formalidad y nivel de supervisión deben responder al contexto real. No es lo mismo aplicar el SGIA en salud, finanzas, educación, seguridad, manufactura o servicios administrativos internos. El sistema debe ser proporcional al nivel de riesgo, al impacto y a las obligaciones del entorno.

## Cierre del módulo 11

Al concluir este módulo, el participante debe comprender que los Anexos B, C y D no son accesorios. El Anexo B ayuda a aterrizar controles. El Anexo C amplía la capacidad de formular objetivos y reconocer riesgos. El Anexo D confirma la posibilidad de adaptar el SGIA a distintos sectores y momentos del ciclo de vida.

En la progresión final del documento, este módulo completa el marco de apoyo a la implementación. El siguiente profundiza en el aseguramiento interno del sistema con referencia metodológica a ISO 19011.

En síntesis, este módulo enseña cómo ISO/IEC 42001 conserva rigor sin perder flexibilidad. Y esa combinación es precisamente una de las razones por las que la norma puede convertirse en un marco de alto valor para certificación, implementación y gobernanza de IA.

# Módulo 12. Aseguramiento interno del SGIA basado en ISO 19011

## Introducción al módulo

En este punto del documento, la atención se desplaza desde la arquitectura de apoyo del sistema hacia la metodología con la que la organización puede revisarse a sí misma con mayor rigor. Este módulo cumple la función de ampliar la dimensión de aseguramiento interno del SGIA.

El material fuente dedica un bloque amplio al aseguramiento interno del SGIA con apoyo en ISO 19011. Este bloque es decisivo para la extensión y el valor pedagógico del documento, por lo que en esta versión debe mantenerse con desarrollo sólido, pero con una semántica más elegante y menos dependiente de una lógica de curso de auditoría tradicional. La idea central no es presentar una actividad punitiva. Es presentar una disciplina de revisión estructurada que permita a la organización generar diagnósticos confiables sobre su sistema y sostener su mejora continua.

ISO 19011 ofrece una base metodológica valiosa para comprender cómo se gestionan programas de revisión, cómo se estructuran actividades de aseguramiento, qué principios protegen la credibilidad del proceso y qué competencias requieren quienes participan en él. Integrar ese enfoque al SGIA resulta especialmente útil porque la IA exige revisiones internas con criterio técnico, sensibilidad al riesgo y capacidad de interpretar evidencia en contextos complejos.

En clave AIMPC™, este módulo fortalece la capacidad de diseñar y ejecutar revisiones internas del SGIA. En clave AIGPC™, ayuda a comprender cómo el órgano de dirección y las funciones de supervisión pueden apoyarse en procesos metodológicamente sólidos para obtener visibilidad sobre el estado del sistema. En ambos casos, el aseguramiento interno actúa como una bisagra entre operación, desempeño y mejora.

## 143. Aseguramiento interno del Sistema de Gestión de IA

El bloque originalmente presentado como Internal Auditor se reinterpreta en este material como un módulo de aseguramiento interno del SGIA basado en los principios de ISO 19011. Su propósito es explicar cómo la organización puede estructurar revisiones internas periódicas para evaluar la consistencia y la eficacia del sistema de acuerdo con ISO/IEC 42001.

Esta reinterpretación ajusta el tono sin perder rigor. La organización no revisa el SGIA únicamente para buscar fallos. Lo revisa para comprender su estado, identificar brechas, validar consistencia, fortalecer trazabilidad y producir información útil para la dirección y

para la mejora. Esa lectura resulta más madura y más alineada con la lógica de un sistema de gestión moderno.

## 144. Enfoque de revisión interna con énfasis en coordinación y proporcionalidad

Basado en ISO 19011, este enfoque ofrece una guía aplicable a organizaciones de todos los tamaños y tipos, así como a revisiones internas de distintos alcances y escalas. Puede aplicarse tanto a revisiones realizadas por equipos amplios como a procesos conducidos por una sola persona, dependiendo de la complejidad del programa y del SGIA.

Este punto tiene mucho valor práctico. Confirma que el aseguramiento del SGIA no necesita un único formato rígido. La organización puede adaptar sus revisiones a su realidad, siempre que mantenga disciplina metodológica, claridad de roles, objetividad suficiente y trazabilidad de resultados. De este modo, el aseguramiento se vuelve sostenible y proporcional.

## 145. Estructura de ISO 19011:2018

La estructura de ISO 19011 incluye prefacio, introducción, alcance, referencias normativas, términos y definiciones, principios de auditoría, gestión de un programa de auditoría, realización de una auditoría, competencia y evaluación de los auditores, además de anexos y bibliografía.

En el contexto del SGIA, esta estructura puede leerse como una ruta metodológica para organizar revisiones internas del sistema. Ayuda a establecer principios, definir programas, estructurar actividades de revisión y comprender las capacidades necesarias para ejecutar un aseguramiento útil y confiable. Su valor radica en ofrecer disciplina metodológica sin imponerse como una camisa de fuerza.

## 146. Alcance de ISO 19011:2018 aplicado al SGIA

ISO 19011 proporciona orientación sobre revisión de sistemas de gestión, incluyendo principios, gestión de programas, realización de revisiones y evaluación de la competencia de las personas involucradas. No reemplaza los requisitos de ISO/IEC 42001, pero sí aporta una base metodológica para organizar el aseguramiento interno del SGIA.

En clave aplicada, esto significa que la organización puede usar ISO 19011 como referencia para dar consistencia a sus revisiones internas, definir criterios de planificación, mejorar la calidad de la recolección de evidencia y fortalecer la credibilidad de las conclusiones obtenidas.

## 147. Revisión estructurada del sistema

La auditoría se define tradicionalmente como un proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla frente a criterios definidos. En esta versión de autoestudio, conviene expresarla como revisión estructurada del sistema.

Esta formulación conserva el rigor del proceso, pero lo aproxima al lenguaje de gestión y aseguramiento. La revisión estructurada del SGIA busca recopilar y analizar información verificable frente a referentes aplicables para emitir un juicio técnicamente defendible sobre la consistencia y eficacia del sistema. Su valor no reside en el formalismo del término, sino en la utilidad del proceso.

## 148. Tipos de revisión del sistema

El material original introduce los tipos de auditoría mediante una clasificación visual. En esta versión, conviene entender esa clasificación como distintos formatos de revisión del sistema según quién la solicita, quién la realiza y con qué propósito se ejecuta.

Esta distinción ayuda a comprender que el SGIA puede ser revisado desde perspectivas internas o externas, y que cada una aporta un valor diferente. Lo relevante, en cualquier caso, es reconocer que todas las revisiones útiles necesitan criterios claros, alcance definido y suficiente independencia funcional respecto del objeto revisado.

## 149. Tipos de revisión del sistema: internas y externas

Las revisiones internas son realizadas por o en nombre de la propia organización. Las revisiones externas incluyen las realizadas por partes con interés en la organización, como clientes, así como las realizadas por organismos independientes, por ejemplo entidades de certificación o autoridades competentes.

Entender esta diferencia ayuda al participante a ubicar el aseguramiento interno dentro de un ecosistema más amplio. La revisión interna fortalece aprendizaje y control desde dentro. La revisión externa puede responder a exigencias contractuales, regulatorias o de certificación. Ambas pueden coexistir y complementarse.

## 150. Referentes de evaluación del SGIA

Los criterios de auditoría se definen como el conjunto de requisitos utilizados como referencia frente a los cuales se compara la evidencia objetiva. En esta versión, puede hablarse de referentes de evaluación del SGIA.

Estos referentes pueden incluir políticas, procedimientos, requisitos de ISO/IEC 42001, obligaciones legales, compromisos contractuales, decisiones de la dirección y otros

elementos pertinentes. Definirlos con claridad es indispensable para cualquier revisión estructurada. Sin referentes, no hay base sólida para emitir conclusiones.

## 151. Artefactos de gestión para la revisión del SGIA

La evidencia objetiva puede entenderse aquí como artefactos de gestión y registros de valor para la revisión del SGIA. Se trata de la información que permite sostener una lectura confiable sobre cómo funciona el sistema, cómo se aplican controles, qué decisiones se han tomado y qué resultados se han observado.

Estos artefactos pueden incluir políticas, procedimientos, matrices de riesgo, resultados de monitoreo, decisiones de dirección, evaluaciones de impacto, planes de tratamiento, registros de remediación, informes internos y cualquier otra información documentada relevante y verificable.

## 152. Resultados de la revisión del SGIA

Los resultados de la revisión del SGIA surgen de contrastar artefactos y registros frente a los referentes definidos. Pueden expresarse como fortalezas, brechas de control, desviaciones del estándar, oportunidades de optimización o buenas prácticas.

Lo decisivo es que el resultado de una revisión no se limite a clasificaciones formales. Debe convertirse en información útil para comprender el estado del sistema y orientar decisiones posteriores.

## 153. Diagnóstico de situación del SGIA

El contenido base incluye referencias a hallazgos, verificación de hechos verbales, notas y redacción de hallazgos. En esta versión, conviene integrar esos elementos bajo la idea de diagnóstico de situación del SGIA.

La organización revisa procesos y controles para confirmar hechos, relacionarlos con criterios aplicables y construir una interpretación técnicamente sólida. El objetivo no es acumular observaciones, sino producir un diagnóstico claro, trazable y accionable.

## 154. Juicio de eficacia del SGIA

Las conclusiones de la revisión pueden entenderse como un juicio de eficacia del SGIA. Se trata de la síntesis interpretativa que surge después de revisar objetivos, criterios, evidencia y resultados.

Este juicio permite responder, de forma razonada, si el sistema se muestra consistente, suficiente y útil para sostener sus resultados previstos. En clave de gobernanza, este tipo de juicio tiene especial valor porque ofrece a la dirección una lectura integrada del estado del SGIA.

## 155. Patrocinador de la revisión del SGIA

El rol que en la terminología tradicional se asocia al cliente de auditoría puede entenderse aquí como patrocinador de la revisión del SGIA. Es quien impulsa o solicita el proceso de revisión y quien, en muchos casos, recibirá sus resultados como insumo para dirección, control o mejora.

Este rol puede estar en la alta dirección, en una función de aseguramiento, en cumplimiento, en calidad o en la coordinación del SGIA. Lo importante es que exista un propósito claro para la revisión y una instancia capaz de dar valor a sus resultados.

## 156. Responsable del proceso revisado

En lugar de hablar de auditado, resulta más apropiado referirse al responsable del proceso revisado o al stakeholder interno vinculado con el ámbito revisado. Esta elección semántica reduce el tono fiscalizador y refuerza una lógica de colaboración y aprendizaje, sin eliminar la claridad sobre quién responde por el proceso evaluado.

## 157. Facilitador de la revisión

La persona que realiza la revisión puede entenderse como facilitador de la revisión estructurada del SGIA. Su papel es conducir el proceso con disciplina metodológica, comparar información frente a referentes definidos, registrar resultados con trazabilidad y contribuir a que la organización obtenga un diagnóstico útil.

Esta formulación preserva la objetividad del rol y, al mismo tiempo, lo sitúa más cerca del lenguaje de gestión y mejora.

## 158. Equipo de aseguramiento del SGIA

El equipo que participa en la revisión puede entenderse como equipo de aseguramiento del SGIA. Puede estar compuesto por una o más personas, según la complejidad del sistema, y puede combinar experiencia metodológica, conocimiento del negocio y apoyo técnico especializado.

Su valor reside en enriquecer la interpretación de resultados, distribuir tareas y sostener revisiones más completas cuando el SGIA abarca múltiples procesos o sistemas de IA.

## 159. Apoyo técnico especializado

El experto técnico puede presentarse como apoyo técnico especializado para la revisión del SGIA. Su función es aportar conocimiento profundo cuando el sistema incluye

componentes complejos, sectores sensibles, tecnologías específicas o requisitos particulares que exigen interpretación experta.

Este apoyo fortalece la calidad del diagnóstico sin sustituir la responsabilidad metodológica de quien conduce la revisión.

## 160. Acompañamiento al proceso de revisión

El rol del observador puede entenderse como figura de acompañamiento al proceso de revisión. Puede responder a necesidades de aprendizaje, supervisión, formación o coordinación interna, sin asumir la conducción del proceso ni la emisión de resultados.

## 161. Facilitación del proceso de revisión

El rol del guía puede reformularse como figura de facilitación del proceso de revisión, designada por la organización para apoyar el acceso a personas, ubicaciones o documentación relevante. Su función es facilitar logística y coordinación, no influir en los resultados.

## 162. Programa de aseguramiento interno del SGIA

El programa de auditoría puede entenderse aquí como programa de aseguramiento interno del SGIA. Se trata del conjunto organizado de revisiones, actividades y seguimientos que la organización planifica en un período determinado para obtener una visión estructurada del estado de su sistema.

Este programa permite priorizar esfuerzos, distribuir recursos y sostener una disciplina periódica de revisión alineada con riesgos, cambios y necesidades de dirección.

## 163. Alcance de la revisión del SGIA

El alcance de la revisión del SGIA corresponde a la delimitación de qué partes del sistema serán analizadas, en qué contextos, sobre qué procesos y durante qué período. Definirlo con claridad es indispensable para asegurar una revisión focalizada, proporcional y útil.

## 164. Plan de revisión del SGIA

El plan de revisión del SGIA organiza cómo se desarrollará la revisión: qué procesos o temas se cubrirán, qué actividades se realizarán, quiénes participarán, qué recursos serán necesarios y cómo se estructurará el trabajo. Es una herramienta de coordinación y de claridad metodológica.

## 165. Alineación con los referentes del sistema

La conformidad puede expresarse aquí como alineación con los referentes del sistema. Esta formulación conserva el sentido técnico de cumplimiento, pero lo presenta desde una óptica más cercana a la gestión y al aseguramiento que a la sanción.

## 166. Desviación del estándar y brecha de control

La no conformidad puede expresarse como desviación del estándar o brecha de control. Esta reformulación mantiene la rigurosidad técnica, pero favorece una lectura orientada a la mejora y a la remediación proporcional.

## 167. Registros de valor para la revisión del sistema

Las pruebas o evidencias verificables pueden integrarse bajo la noción de registros de valor para la revisión del sistema. Estos registros conectan observaciones con referentes aplicables y sostienen la credibilidad del diagnóstico.

## 168. Métodos para la revisión del sistema

Los métodos de revisión corresponden a las formas en que la organización recopila, contrasta y analiza información para comprender el funcionamiento del SGIA. Pueden combinar revisión documental, entrevistas, observación, muestreo y contraste de evidencia. La selección adecuada de métodos fortalece profundidad, eficiencia y trazabilidad.

## 169. Principios de aseguramiento del SGIA

El material base presenta los principios de auditoría: integridad, presentación justa, debido cuidado profesional, confidencialidad, independencia, enfoque basado en la evidencia y enfoque basado en el riesgo. En esta versión, pueden entenderse como principios de aseguramiento del SGIA.

Estos principios son condiciones de confianza. Permiten que una revisión sea creíble, útil y técnicamente sólida. Sin ellos, el proceso pierde legitimidad y sus resultados dejan de ser una base segura para la mejora del sistema.

## 170. Principios de aseguramiento del SGIA: integridad

La integridad constituye la base del profesionalismo. En el contexto del SGIA, significa actuar con honestidad, responsabilidad, imparcialidad y sensibilidad frente a influencias que puedan distorsionar el juicio. Este principio da legitimidad a la revisión y protege la credibilidad de sus resultados.

## 171. Principios de aseguramiento del SGIA: presentación clara y fiel

La presentación justa puede entenderse como una presentación clara y fiel del diagnóstico del SGIA. Los resultados deben comunicarse de forma veraz, precisa, objetiva, oportuna, clara y completa. Solo así pueden convertirse en insumo real para la dirección y para la mejora.

## 172. Principios de aseguramiento del SGIA: debido cuidado profesional

El debido cuidado profesional implica aplicar diligencia, criterio técnico y juicio razonado durante la revisión. En un SGIA, donde los riesgos e impactos de IA pueden ser complejos, este principio resulta indispensable para evitar interpretaciones superficiales o conclusiones apresuradas.

## 173. Principios de aseguramiento del SGIA: confidencialidad

La confidencialidad exige proteger adecuadamente la información obtenida durante la revisión. En el SGIA pueden aparecer datos sensibles sobre riesgos, incidentes, controles, decisiones o relaciones con terceros. Su tratamiento responsable forma parte de la calidad del proceso de aseguramiento.

## 174. Principios de aseguramiento del SGIA: objetividad e independencia

La independencia puede leerse aquí como necesidad de objetividad e independencia funcional. La organización debe procurar que quienes conduzcan revisiones mantengan suficiente distancia respecto del objeto revisado para evitar sesgos o conflictos que afecten la credibilidad del proceso.

## 175. Principios de aseguramiento del SGIA: enfoque basado en registros de valor

El enfoque basado en la evidencia puede expresarse como un enfoque basado en registros de valor y artefactos de gestión verificables. La revisión debe apoyarse en información confiable, trazable y relevante. Ese soporte da solidez al diagnóstico y al juicio de eficacia del sistema.

## 176. Principios de aseguramiento del SGIA: enfoque basado en riesgo

El enfoque basado en el riesgo puede entenderse como una priorización del aseguramiento por criticidad y contexto. La revisión debe concentrarse en aquello que

más afecta la capacidad del SGIA para alcanzar resultados previstos: procesos críticos, controles relevantes, áreas sensibles, cambios significativos e impactos potenciales.

## Integración metodológica del módulo 12

Este módulo no debe leerse como un bloque ajeno al resto del documento. Es una prolongación natural de la cláusula 9 y un soporte metodológico para la cláusula 10. La revisión estructurada del SGIA alimenta la evaluación del desempeño, fortalece la revisión por la dirección y produce información útil para la mejora continua.

En clave de certificación, su valor es doble. Por un lado, ayuda a que el participante comprenda cómo se organiza el aseguramiento interno del sistema. Por otro, le enseña a interpretar la revisión no como inspección punitiva, sino como un mecanismo de disciplina, aprendizaje y visibilidad institucional.

## Cierre del módulo 12

Al finalizar este módulo, el participante debe comprender que el aseguramiento interno del SGIA es una práctica esencial para sostener confianza en el sistema. A través de una revisión estructurada, basada en principios claros, criterios definidos, roles adecuados y evidencia verificable, la organización puede diagnosticar su estado, fortalecer su trazabilidad y orientar su mejora.

En la lógica del documento, este módulo prepara el cierre integrador. Una vez comprendidos los fundamentos, las cláusulas, los anexos y la revisión estructurada del sistema, el participante está listo para consolidar una lectura completa del SGIA.

En síntesis, este módulo aporta una idea central para el profesional senior: un SGIA maduro no solo diseña y opera controles. Además se observa a sí mismo con método, objetividad y propósito de fortalecimiento continuo.

# Módulo 13. Cierre del material de estudio

## Introducción al cierre

Este último módulo no abre una temática nueva. Su función es integrar todo lo recorrido y devolver al lector una lectura unificada del sistema. Actúa como cierre pedagógico y como consolidación estratégica del documento.

Después de recorrer fundamentos, cláusulas, anexos y aseguramiento interno del SGIA, el participante necesita consolidar una lectura final del sistema. El cierre del material no debe reducirse a una recapitulación mecánica. Debe ofrecer una síntesis de sentido. Debe mostrar cómo todas las piezas estudiadas se articulan dentro de una misma arquitectura de gestión y por qué esa arquitectura tiene valor estratégico, operativo y comercial en el contexto actual de la inteligencia artificial.

Además resulta importante que el cierre corrija posibles interpretaciones erróneas. Uno de los riesgos frecuentes en la formación sobre normas de gestión es trasladar de manera automática lógicas de otros estándares sin atender a la especificidad de la IA. Este documento debe evitar esa confusión y reforzar que ISO/IEC 42001 es una norma de sistema de gestión de inteligencia artificial, no una simple extensión de seguridad de la información ni una norma exclusivamente tecnológica.

## Síntesis integradora del SGIA

A lo largo de este material, el SGIA se ha presentado como una estructura que conecta contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua. Esa secuencia responde al ciclo PHVA y ofrece a la organización una forma disciplinada de gobernar la IA.

El contexto define la realidad en la que el sistema operará. El liderazgo establece dirección, prioridad y compromiso. La planificación convierte esa dirección en decisiones explícitas sobre riesgos, impactos, objetivos y cambios. El soporte dota al sistema de recursos, competencias, comunicación y trazabilidad documental. La operación materializa controles y procesos. La evaluación del desempeño convierte la experiencia del sistema en información útil. La mejora continua transforma esa información en evolución estructurada.

Este recorrido demuestra que ISO/IEC 42001 no se limita a una lógica de revisión de cumplimiento. Más bien construye una capacidad institucional para gestionar la IA con consistencia, responsabilidad y visión de largo plazo. Ese es, precisamente, el gran valor del SGIA: convertir la IA en una capacidad gobernable.

## Valor profesional para AIMPC™ y AIGPC™

Desde la lógica de AIMPC™, el documento proporciona la base para diseñar, implementar, coordinar y sostener un SGIA funcional. Ayuda a comprender cómo se definen procesos, controles, responsabilidades, métricas, documentación y mecanismos de tratamiento del riesgo e impacto. En otras palabras, forma al profesional capaz de materializar el sistema.

Desde la lógica de AIGPC™, el documento amplía esa capacidad hacia la gobernanza. Permite comprender por qué la alta dirección debe involucrarse, cómo se articula la revisión por la dirección, qué significa aceptar riesgo residual, por qué la evaluación de impacto tiene una dimensión social y cómo el órgano de gobierno puede ejercer supervisión real sobre el uso de IA dentro de la organización.

La integración de ambas perspectivas es uno de los grandes diferenciales de este material. La operación sin gobierno fragmenta. La gobernanza sin operación se vuelve declarativa. El profesional senior necesita dominar ambas dimensiones para aportar verdadero valor a la organización.

## Precisión final sobre el alcance del documento

Este material se centra en la gestión de inteligencia artificial conforme a ISO/IEC 42001. Aunque algunos de sus controles y decisiones dialogan con otras capacidades organizacionales como seguridad de la información, privacidad, calidad, cumplimiento o continuidad, el foco del documento es el SGIA. Esa precisión resulta importante para evitar una lectura reductiva o una asimilación automática con otros sistemas de gestión.

La IA introduce particularidades que justifican un tratamiento específico: dependencia de datos, opacidad de ciertos resultados, cambios en comportamiento, sensibilidad al contexto de uso, impacto potencial sobre individuos y sociedad, y exigencias crecientes de rendición de cuentas. ISO/IEC 42001 organiza una respuesta a esas particularidades. No se limita a repetir la lógica de otros estándares. La adapta al hecho de que la IA requiere una gobernanza proporcional a su complejidad y a sus consecuencias.

## Conclusión final

La implementación de un SGIA conforme a ISO/IEC 42001 representa una decisión estratégica. Permite a la organización tratar la IA con una disciplina comparable a la que utiliza para otras capacidades críticas, pero ajustada a los desafíos propios de esta tecnología. Ese tratamiento fortalece confianza, trazabilidad, coherencia y capacidad de respuesta.

Para el profesional que se prepara en AIMPC™ y AIGPC™, el valor del documento radica en ofrecer una lectura completa, integrada y aplicable del sistema. No se limita a exponer

requisitos. Enseña una manera de pensar la IA dentro de la organización, de diseñarla, gobernarla, revisar su desempeño y mejorarla con criterio. En el contexto actual, eso no constituye solo una ventaja técnica. Representa también una ventaja competitiva y una señal clara de madurez institucional.

## Cierre del módulo 13

Con este cierre, el participante debería estar en condiciones de leer ISO/IEC 42001 no como una colección de cláusulas independientes, sino como una arquitectura coherente de gestión y gobernanza de IA. Esa comprensión es la base sobre la cual se sostiene tanto la certificación como la aplicación real del sistema en organizaciones de distintos sectores y niveles de madurez.

# ¿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 **ATP (Authorized Training Partner).**
- **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 está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

# Nuestras Afiliaciones

# Aprendizaje Permanente

Certiprof ha creado una insignia especial **Lifelong Learning** 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:

**https://certiprof.com/pages/certiprof-lifelong-learning**

# COMPARTE Y VERIFICA **TUS LOGROS DE APRENDIZAJE** FÁCILMENTE

#AIGPC #certiprof



certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com