ISO/IEC 42001

FOUNDATION

PROFESSIONAL CERTIFICATION

certiprof®

I42001F™ VERSIÓN 042026

MÓDULO 0 – INTRODUCCIÓN

Bienvenida a la Certificación I42001F™

En un entorno donde la inteligencia artificial transforma modelos de negocio, procesos operativos y decisiones estratégicas, las organizaciones ya no pueden depender de prácticas informales para su gestión. Se requieren estructuras formales que permitan gobernar la IA con criterios de responsabilidad, trazabilidad y control.

La certificación **ISO/IEC 42001 Foundation Professional Certification (I42001F™)** introduce los fundamentos del Sistema de Gestión de Inteligencia Artificial (SGIA), conforme a la norma internacional **ISO/IEC 42001:2023**. Este nivel valida la comprensión estructural y conceptual del estándar, permitiendo interpretar su propósito, su terminología esencial y la arquitectura general del sistema.

Foundation no evalúa implementación avanzada ni auditoría, sino claridad conceptual. Este material constituye un recurso de apoyo recomendado para estructurar el estudio, aunque no es obligatorio para presentar el examen.

Autoevaluación: ¿Podrías explicar en una frase qué valida el nivel Foundation frente a niveles más avanzados?

Propósito de esta Guía de Autoestudio

Comprender una norma de sistema de gestión exige más que leer requisitos aislados; implica entender su lógica interna y la interrelación entre sus componentes. Esta guía organiza el contenido de ISO/IEC 42001 en una secuencia didáctica alineada con el blueprint oficial del examen, facilitando la comprensión integral de los capítulos 4–10, la Declaración de Aplicabilidad (SoA) y los anexos A y B.

El objetivo no es memorizar cláusulas, sino desarrollar criterio para ubicar cada concepto dentro del sistema de gestión. La comprensión estructural permite responder con seguridad a escenarios conceptuales y distinguir entre requisitos obligatorios, controles de referencia y orientación complementaria.

Autoevaluación: ¿Tu enfoque de estudio prioriza comprender la arquitectura del sistema o memorizar textos normativos?

Alcance del Nivel Foundation

Antes de profundizar en la norma, es esencial delimitar su alcance en este nivel. La certificación Foundation valida la capacidad de definir terminología clave del SGIA, explicar el propósito del sistema, describir la estructura de los capítulos 4–10, comprender el rol estratégico de la SoA e identificar anexos pertinentes ante escenarios básicos.

No certifica competencias de auditoría formal, ni implementación técnica detallada, ni diseño específico de controles. Se trata de una certificación de comprensión estructural que constituye la base para niveles posteriores.

Esta claridad evita expectativas erróneas y orienta adecuadamente el estudio.

Autoevaluación: ¿Puedes diferenciar claramente entre comprender la norma y auditarla formalmente?

Perfil Profesional I42001F™

Este nivel está dirigido a profesionales de GRC (Gobierno, Riesgo y Cumplimiento), cumplimiento normativo, calidad, procesos, gestión de proyectos, producto digital, riesgo o transformación organizacional que requieren un lenguaje común técnico–negocio en materia de IA.

No exige programación, experiencia previa en auditoría ni implementación de normas ISO**. ISO/IEC 42001** no es una norma técnica de modelado algorítmico; es un marco organizacional que establece cómo gestionar sistemas de IA dentro de una estructura formal de gobernanza.

Su valor radica en facilitar el diálogo entre áreas técnicas y áreas estratégicas bajo un marco normativo común.

Autoevaluación: ¿Cómo puede esta certificación fortalecer tu capacidad de diálogo con áreas técnicas o de cumplimiento?

Arquitectura del Examen I42001F™

Comprender cómo serás evaluado permite orientar el estudio con estrategia. El examen consta de 40 preguntas de opción múltiple, 60 minutos de duración y una puntuación mínima de aprobación aproximada del 80 %.

La distribución por dominios otorga mayor peso a la estructura de la norma (40 %), seguida de terminología y propósito (25 %), SoA y anexos (20 %), roles y aplicabilidad (10 %) e interpretación básica en escenarios (5 %).

Este enfoque confirma que dominar la arquitectura del estándar es más relevante que memorizar detalles secundarios.

Autoevaluación: ¿En qué dominio deberías invertir más tiempo según su peso porcentual?

Estrategia de Estudio para Foundation

Dado que el examen evalúa la comprensión estructural, la estrategia de estudio debe centrarse en asociar cada concepto con su capítulo correspondiente. Más que memorizar numerales, es fundamental reconocer relaciones como política → liderazgo, riesgos → planificación, no conformidad → mejora, y revisión por la dirección → evaluación del desempeño.

La práctica con escenarios conceptuales fortalece la capacidad de ubicar correctamente los temas dentro del ciclo del SGIA. Comprender la secuencia lógica del sistema permite responder con precisión incluso cuando la pregunta esté formulada de manera indirecta.

💡 **TIP DE EXAMEN:** Cuando una pregunta mencione política, objetivos, auditoría, no conformidad o revisión por la dirección, ubica primero el capítulo antes de analizar las opciones. Esa asociación reduce errores por distractores conceptuales.

Autoevaluación: Si te mencionan "revisión por la dirección", ¿puedes ubicar su capítulo sin consultar la norma?

¿Qué es ISO/IEC 42001?

ISO/IEC 42001 es una norma internacional que establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Inteligencia Artificial. Su enfoque no es técnico-operativo sobre algoritmos, sino organizacional: define cómo gobernar la IA dentro de una estructura formal.

Comparte la lógica de otras normas como **ISO 9001** o **ISO 27001**, aplicando la estructura armonizada ISO al contexto específico de la IA. Esto facilita su integración con sistemas existentes y refuerza la coherencia en la gestión organizacional.

La norma se centra en procesos, responsabilidades, evaluación del riesgo y mejora continua.

Autoevaluación: ¿Cuál es la diferencia entre gestionar IA y desarrollar técnicamente un modelo de IA?

Estructura General de la Norma

La norma se organiza en capítulos que siguen la estructura de alto nivel ISO: contexto, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora.

Los capítulos 4–10 contienen los requisitos obligatorios para la certificación. Los anexos complementan estos requisitos con controles de referencia y orientación para su implementación.

El examen se enfoca especialmente en los capítulos 4–10 y en los anexos A y B. Reconocer esta arquitectura es indispensable para interpretar correctamente cualquier pregunta conceptual.

Autoevaluación: ¿Puedes enumerar mentalmente los capítulos del 4 al 10 en orden lógico?

Integración con Otros Sistemas de Gestión

La estructura armonizada permite integrar el SGIA con sistemas existentes como ISO 9001, ISO 27001 o ISO 27701. Esto facilita la gestión coordinada de políticas, riesgos, auditorías internas y revisiones por la dirección.

La integración reduce duplicidades documentales, optimiza recursos y fortalece la gobernanza organizacional frente a la IA. No se trata de crear un sistema paralelo, sino de ampliar el marco existente para incorporar la gestión específica de la inteligencia artificial.

Autoevaluación: ¿Tu organización podría integrar el SGIA con un sistema de gestión ya implementado?

Lógica del Ciclo del SGIA

El **SGIA** responde a una lógica secuencial coherente con el ciclo de mejora continua: comprender el contexto, definir liderazgo y política, planificar riesgos y objetivos, proveer soporte y recursos, operar procesos, evaluar desempeño y mejorar continuamente.

Este flujo refleja el principio estructural de los sistemas de gestión ISO. Cada fase alimenta a la siguiente y permite que la organización mantenga control dinámico sobre sus sistemas de IA.

Autoevaluación: Si se detecta una no conformidad, ¿en qué parte del ciclo estamos actuando?

DOMINIO A – TERMINOLOGÍA Y PROPÓSITO

Dominio A – Terminología y Propósito

Con el panorama general establecido, el siguiente paso es dominar el lenguaje del SGIA. El Dominio A del examen evalúa la capacidad de comprender terminología clave y explicar el propósito y la aplicabilidad de la norma.

Sin un uso correcto de términos como riesgo, control, impacto o SoA, la interpretación del estándar pierde precisión. La claridad conceptual no es un detalle académico: es una condición para aplicar correctamente los requisitos.

Este dominio constituye la base sobre la cual se construye la comprensión de los capítulos normativos.

Autoevaluación: ¿Podrías definir SGIA con claridad y sin ambigüedades?

Precisión Terminológica en ISO

En las normas ISO, cada término tiene un significado específico y no intercambiable. Confundir riesgo con control, o corrección con acción correctiva, puede generar errores sustantivos de interpretación.

La precisión conceptual es evaluable en el examen Foundation y esencial en contextos de implementación o auditoría. El uso adecuado del lenguaje refleja la comprensión real del sistema.

Dominar la terminología implica entender su función dentro del ciclo de gestión y su relación con los requisitos normativos.

⚠ **ALERTA DE ERROR:** Corrección y acción correctiva no son equivalentes. La corrección elimina la no conformidad detectada; la acción correctiva elimina la causa para evitar su recurrencia.

Autoevaluación: ¿Sabes explicar con claridad la diferencia entre corrección y acción correctiva?

¿Por qué un SGIA?

La adopción de IA genera oportunidades de innovación, eficiencia y escalabilidad. Sin embargo, también introduce riesgos técnicos, regulatorios, éticos y reputacionales.

El SGIA proporciona una estructura sistemática para identificar, evaluar, tratar y monitorear esos riesgos. Permite a la organización demostrar control, responsabilidad y coherencia en la gestión de sistemas de IA.

En entornos regulados o de alta exposición pública, gobernar la IA no es opcional; es una necesidad estratégica.

Autoevaluación: ¿Qué tipo de riesgo asociado a IA podría impactar directamente a tu organización?

SGIA vs Desarrollo Técnico

Es esencial diferenciar entre el desarrollo técnico de modelos y la gestión organizacional de la IA. ISO/IEC 42001 no prescribe algoritmos, arquitecturas ni métodos de entrenamiento; prescribe responsabilidades, procesos, controles y mecanismos de supervisión.

El **SGIA** gobierna el ciclo de vida del sistema de IA desde una perspectiva organizacional. Esta distinción evita confusiones tanto en el examen como en la práctica profesional.

Autoevaluación: ¿Puedes explicar esta diferencia a alguien sin formación técnica?

Aplicabilidad de la Norma

ISO/IEC 42001 aplica a organizaciones que desarrollan, proveen o utilizan sistemas de IA, independientemente de su tamaño o sector.

La aplicabilidad depende de la relación con la IA, no del tipo de industria. Incluso una organización que solo utilice soluciones de IA desarrolladas por terceros puede requerir un SGIA para gestionar su uso responsable.

Autoevaluación: ¿Tu organización entra dentro del alcance potencial de la norma?

Roles Organizacionales Frente a la IA

El rol organizacional —proveedor, desarrollador, integrador o usuario— influye en la aplicabilidad de requisitos y controles del SGIA.

Comprender estos roles permite interpretar correctamente los escenarios planteados en el examen y delimitar responsabilidades dentro de la organización.

La responsabilidad nunca desaparece; solo cambia su alcance según el nivel de intervención sobre el sistema de IA.

Autoevaluación: ¿En qué rol principal se ubica tu organización respecto a la IA?

Mejora Continua en el SGIA

La IA evoluciona constantemente. Nuevos datos, nuevos contextos regulatorios y nuevos usos pueden modificar el perfil de riesgo.

Por ello, el **SGIA** incorpora mecanismos de evaluación del desempeño, auditoría interna y acción correctiva que permiten mantener su eficacia.

La mejora continua no implica cambio constante de tecnología, sino optimización sistemática del marco de gestión.

Autoevaluación: ¿Por qué la mejora continua es especialmente relevante en contextos de IA?

Declaración de Aplicabilidad (SoA)

La **SoA** documenta los controles necesarios y justifica su inclusión o exclusión en función de los riesgos identificados.

Es un elemento central de trazabilidad dentro del **SGIA,** ya que conecta evaluación de riesgos con decisiones de control.

No es un checklist genérico; es un documento estratégico que refleja análisis contextualizado.

Autoevaluación: ¿Qué implicación tendría excluir un control sin justificarlo adecuadamente?

Anexo A y Anexo B

El Anexo A proporciona controles de referencia.

El Anexo B ofrece orientación para su implementación.

La organización determina la aplicabilidad de los controles según su contexto y evaluación de riesgos. Diferenciar entre requisito obligatorio y control de referencia es un punto frecuente de evaluación en el examen.

Autoevaluación: ¿En qué anexo encontrarías orientación práctica para aplicar un control específico?

Cierre del Módulo 0

Con esta base conceptual, ya comprendes qué es **ISO/IEC 42001**, qué certifica el nivel Foundation, cómo se estructura el examen y cuál es la lógica general del SGIA.

El siguiente bloque profundizará en la terminología formal del sistema y su aplicabilidad organizacional, consolidando la arquitectura conceptual necesaria para interpretar correctamente los capítulos normativos.

Autoevaluación: ¿Puedes explicar el ciclo completo del SGIA sin apoyo visual?

MÓDULO 1 – DOMINIO A

Sistema de Gestión de Inteligencia Artificial (SGIA)

Un **Sistema de Gestión de Inteligencia Artificial (SGIA**) es el conjunto de elementos interrelacionados que permiten establecer políticas, objetivos y procesos para gestionar sistemas de IA dentro de una organización. **ISO/IEC 42001** adopta la estructura armonizada de las normas ISO para definir requisitos que aseguren que la IA se gestiona de forma estructurada, controlada y alineada con el contexto organizacional.

Conviene subrayarlo: un sistema de gestión no es solo documentación. Incluye liderazgo, planificación, operación, evaluación y mejora. Dicho de otro modo, el SGIA convierte la gestión de IA en una disciplina verificable: define cómo se decide, cómo se controla y cómo se mejora.

🔍 **CASO PRÁCTICO:** Si una empresa desarrolla modelos de scoring crediticio, el SGIA no es el modelo en sí, sino el sistema organizacional que gobierna cómo se diseña, valida, monitorea y mejora ese modelo.

Autoevaluación: ¿Podrías explicar la diferencia entre un modelo de IA y el sistema de gestión que lo gobierna?

Propósito de ISO/IEC 42001

El propósito de ISO/IEC 42001 es especificar requisitos para establecer, implementar, mantener y mejorar continuamente un SGIA. La norma no regula algoritmos específicos; regula cómo la organización gestiona los riesgos, impactos y responsabilidades asociados al uso de IA. Su enfoque es organizacional y sistémico.

Lo esencial aquí es la intención: asegurar que la IA se gobierne con criterios de responsabilidad y control, integrados en procesos reales y no como iniciativas aisladas. Por eso, el estándar se alinea con el enfoque de mejora continua propio de los sistemas de gestión ISO.

Ejemplo aplicado: una organización puede usar distintos algoritmos, pero todos deben estar bajo un mismo marco de gobernanza definido por el SGIA.

Autoevaluación: ¿ISO/IEC 42001 regula directamente la arquitectura técnica del modelo?

Alcance del SGIA

El alcance del SGIA define los límites y la aplicabilidad del sistema de gestión dentro de la organización. Debe considerar actividades relacionadas con IA, unidades organizacionales incluidas y sistemas de IA cubiertos.

El alcance debe ser coherente con el contexto organizacional y, además, debe sostenerse con justificación documental. Un alcance claro evita ambigüedades: define qué se gestiona, con qué límites y bajo qué responsabilidades. En certificación, es un punto sensible, porque determina el territorio del SGIA.

Ejemplo aplicado: una empresa podría incluir en su alcance únicamente los sistemas de IA utilizados en atención al cliente, si así lo justifica documentalmente.

Autoevaluación: ¿Es válido definir un alcance limitado sin justificación formal?

Contexto de la Organización

El contexto de la organización incluye factores internos y externos que afectan la capacidad del SGIA para lograr los resultados previstos.

Factores externos: regulación, mercado, tecnología.

Factores internos: cultura, recursos, estructura organizacional.

Este análisis no es una formalidad: establece el punto de partida de la gobernanza. Cambios en el entorno, por ejemplo, regulación emergente o presión reputacional, pueden redefinir prioridades y riesgos, y con ello ajustar el enfoque del SGIA.

Ejemplo aplicado: una regulación emergente sobre transparencia algorítmica constituye un factor externo que impacta el SGIA.

Autoevaluación: ¿Cómo influye el entorno regulatorio en la definición del SGIA?

Partes Interesadas

Una parte interesada es una persona u organización que puede afectar o verse afectada por decisiones relacionadas con IA. Pueden ser clientes, reguladores, empleados y usuarios finales.

Identificar partes interesadas es un requisito del capítulo 4. La razón es directa: la IA puede generar impactos diferenciados, y la organización debe reconocer quiénes están en el perímetro de afectación y qué expectativas o requisitos relevantes existen. Esto incluye requisitos legales, contractuales o de confianza pública.

Ejemplo aplicado: un cliente cuya solicitud de crédito es rechazada por un modelo automatizado es una parte interesada directa.

Autoevaluación: ¿Un proveedor externo de datos podría considerarse parte interesada?

Política de IA

La política de IA expresa la intención y dirección de la organización respecto a la gestión de la IA. Debe ser aprobada por la Alta Dirección, ser comunicada y ser coherente con el contexto.

La política es el marco para establecer objetivos y, sobre todo, para alinear decisiones: no es un texto aspiracional, sino un compromiso verificable que orienta prioridades, responsabilidades y criterios de gobernanza. Cuando la política es clara, el SGIA gana coherencia; cuando es vaga, el sistema se vuelve interpretativo y frágil.

Ejemplo aplicado: una política puede declarar el compromiso con el uso responsable y transparente de IA.

Autoevaluación: ¿Puede existir un SGIA sin una política formal documentada?

Objetivos de IA

Los objetivos de IA deben ser coherentes con la política y, cuando sea posible, medibles. Contribuyen a reducir riesgos, mejorar desempeño y asegurar cumplimiento.

Los objetivos convierten la política en dirección operativa. Para un SGIA, objetivo no equivale a intención: implica definición, seguimiento y evidencia. Si no existe trazabilidad entre política y objetivos, la gobernanza pierde control práctico.

Ejemplo aplicado: "Reducir en un 20 % las desviaciones detectadas en validaciones de modelos" es un objetivo medible.

Autoevaluación: ¿Un objetivo sin indicador asociado es suficientemente verificable?

Riesgo en el SGIA

El riesgo es el efecto de la incertidumbre sobre los objetivos. En el contexto de IA, puede incluir sesgos, impactos éticos, incumplimiento regulatorio y riesgo reputacional.

La gestión del riesgo es central en el SGIA porque conecta intención (objetivos) con control (decisiones de mitigación). No se trata de evitar problemas, sino de comprenderlos, priorizarlos y gestionarlos de forma consistente. En IA, el riesgo suele ser multidimensional: técnico, legal, social y operativo.

Ejemplo aplicado: un modelo que discrimina indirectamente por variables correlacionadas representa un riesgo organizacional.

Autoevaluación: ¿El riesgo en IA puede ser tanto técnico como reputacional?

Tratamiento del Riesgo

El tratamiento del riesgo implica seleccionar opciones para modificar riesgos identificados. Puede incluir implementar controles, evitar el riesgo o aceptarlo con justificación.

El tratamiento debe documentarse formalmente. El punto clave es que la organización toma una decisión explícita frente al riesgo: no lo ignora. Además, el tratamiento no es una acción única; requiere seguimiento para verificar si el riesgo residual es aceptable.

Ejemplo aplicado: si el riesgo es alto sesgo, el tratamiento puede ser introducir validaciones adicionales.

Autoevaluación: ¿Es obligatorio eliminar todos los riesgos identificados?

Control

Un control es una medida que mantiene o modifica un riesgo. Puede ser preventivo, detectivo o correctivo.

Los controles pueden derivarse del Anexo A o ser diseñados por la organización. En un SGIA, el control debe estar definido, implementado y revisado en términos de eficacia. Un control en papel no reduce riesgo; solo lo hace un control operativo y verificable.

Ejemplo aplicado: la revisión periódica independiente del modelo es un control detectivo.

Autoevaluación: ¿Un control necesariamente elimina completamente el riesgo?

Declaración de Aplicabilidad (SoA)

La **SoA** documenta los controles necesarios y justifica su inclusión o exclusión. Conecta riesgos, controles seleccionados y justificación.

Es un documento clave del SGIA porque demuestra trazabilidad y racionalidad en la selección de controles. Dicho esto, la SoA no es un listado genérico: refleja decisiones contextualizadas. En certificación, una SoA sólida evidencia que el tratamiento del riesgo fue real y que la organización entiende su contexto.

Ejemplo aplicado: si un control del Anexo A no aplica porque no se desarrolla internamente el modelo, debe justificarse en la SoA.

Autoevaluación: ¿La SoA es obligatoria aun si todos los controles son aplicables?

No Conformidad

Una no conformidad es el incumplimiento de un requisito del SGIA o de la norma. Puede surgir de auditorías, revisiones internas o evaluaciones regulatorias y debe gestionarse formalmente.

La no conformidad no es un error menor; es una señal de que el sistema no está cumpliendo lo establecido. En sistemas de gestión, lo relevante es cómo se responde: corrección, análisis de causa y acciones para evitar recurrencia, con evidencia documentada.

Ejemplo aplicado: no documentar la revisión anual del SGIA constituye una no conformidad.

Autoevaluación: ¿Toda no conformidad implica sanción externa?

Corrección y Acción Correctiva

Corrección: eliminar la no conformidad detectada. Acción correctiva: eliminar la causa para evitar su recurrencia.

Ambas forman parte del capítulo 10 (Mejora). Esta distinción es esencial: corregir resuelve el síntoma; la acción correctiva evita que el problema se repita. En certificación, se evalúa si la organización es capaz de demostrar gestión sistemática, no solo reacción puntual.

Ejemplo aplicado: actualizar un procedimiento es corrección; rediseñar el proceso de supervisión es acción correctiva.

Autoevaluación: ¿Corregir sin analizar la causa cumple totalmente el requisito?

Seguimiento y Medición

Seguimiento: determinar el estado de un proceso.

Medición: asignar un valor cuantitativo.

Ambos permiten evaluar el desempeño del SGIA y generar evidencia objetiva. Medir sin interpretar no aporta control; seguir sin datos puede volverse subjetivo. El equilibrio es clave: indicadores con análisis, y análisis con decisiones.

Ejemplo aplicado: medir la tasa de errores del modelo es medición; analizar su tendencia es seguimiento y análisis.

Autoevaluación: ¿Medir sin analizar resultados aporta mejora?

Evaluación del Desempeño

La evaluación del desempeño determina el grado en que el SGIA logra resultados previstos. Incluye indicadores, auditoría interna y revisión por la dirección.

Es requisito del capítulo 9. La evaluación del desempeño no se limita al rendimiento técnico del sistema de IA; evalúa la eficacia del sistema de gestión: si los procesos funcionan, si los controles son eficaces y si se cumplen los requisitos definidos.

Ejemplo aplicado: una auditoría interna anual del SGIA forma parte de la evaluación del desempeño.

Autoevaluación: ¿La auditoría interna evalúa personas o evalúa el sistema?

Mejora Continua

La mejora continua busca incrementar la idoneidad, adecuación y eficacia del SGIA. No implica necesariamente innovación tecnológica, sino optimización sistemática del sistema de gestión.

En IA, la mejora continua es especialmente relevante porque los modelos, los datos y los contextos de uso cambian. La organización debe ajustar procesos y controles para mantener la eficacia del SGIA a lo largo del tiempo.

Ejemplo aplicado: actualizar criterios de validación tras detectar desviaciones es mejora continua.

Autoevaluación: ¿Mejora continua significa cambiar constantemente la tecnología?

Aplicabilidad de ISO/IEC 42001

La norma aplica a organizaciones que desarrollan IA, proveen IA o usan IA.

No depende del tamaño ni del sector. El criterio es la relación con sistemas de IA. Por ello, una organización que use IA de terceros no queda exenta: debe gobernar su uso, sus riesgos y sus responsabilidades dentro de su propio contexto.

Autoevaluación: ¿Solo los desarrolladores de IA pueden aplicar ISO/IEC 42001?

Diferencia entre SGIA y Desarrollo Técnico

El SGIA gestiona responsabilidades, riesgos y controles organizacionales; el desarrollo técnico se ocupa de algoritmos y datos. ISO/IEC 42001 aborda el primero.

Este punto es crítico para evitar interpretaciones erróneas: la norma no prescribe cómo entrenar modelos, sino cómo gobernar su ciclo de vida desde el punto de vista organizacional, asegurando control, evidencia, supervisión y mejora.

⚠ **ALERTA DE ERROR:** No confundas sistema de IA con sistema de gestión. El primero es el objeto gestionado; el segundo es la estructura organizacional que lo gobierna.

Ejemplo aplicado: el SGIA define quién valida el modelo; el equipo técnico define cómo se entrena.

Autoevaluación: ¿Puede existir buen desarrollo técnico sin gobernanza formal?

Relación entre Conceptos Clave

En el **SGIA**, los conceptos se conectan en una secuencia lógica: contexto → identificación de riesgos → tratamiento → selección de controles → SoA → evaluación → mejora.

Estos elementos no funcionan de forma aislada. La fuerza del sistema está en su coherencia: el contexto define prioridades, el riesgo determina decisiones de control, la SoA evidencia selección, y la evaluación permite mejorar continuamente.

Ejemplo aplicado: un cambio regulatorio, como contexto, genera nuevos riesgos que deben reflejarse en la SoA.

Autoevaluación: ¿Podrías explicar esta secuencia lógica sin apoyo visual?

Cierre del Dominio A

El Dominio A evalúa comprensión terminológica y propósito del SGIA. Dominar SGIA, riesgo, control, SoA, no conformidad, política y mejora es esencial para responder correctamente preguntas conceptuales del examen. Este dominio no es introductorio en el sentido simple: es la base que sostiene la interpretación de todo el estándar. Sin precisión terminológica, el resto de la norma se entiende de manera fragmentada.

Autoevaluación: ¿Te sientes capaz de definir cada término sin ambigüedad?

MÓDULO 2 – DOMINIO B

Estructura Armonizada (HLS) en ISO/IEC 42001

ISO/IEC 42001 adopta la Estructura Armonizada de las normas de sistemas de gestión (Harmonized Structure, HS), común en estándares como ISO 27001 e ISO 9001. Esto implica que los capítulos 4 al 10 siguen una secuencia estable: Contexto, Liderazgo, Planificación, Soporte, Operación, Evaluación del desempeño y Mejora.

La ventaja es doble. Por un lado, facilita el aprendizaje: una vez comprendes la lógica de la HLS, puedes navegar la norma con mayor precisión. Por otro, habilita la integración: el SGIA no se gestiona como un sistema aislado, sino como un componente que puede

alinearse con sistemas existentes, como calidad, seguridad y privacidad, compartiendo prácticas como auditorías internas, revisión por la dirección y gestión del riesgo.

Ejemplo aplicado: una organización con ISO 27001 puede integrar el SGIA utilizando procesos ya existentes de auditoría, revisión por la dirección y gestión de riesgos.

Autoevaluación: ¿Por qué ISO utiliza una estructura armonizada en sus normas de gestión?

Capítulo 4 – Contexto de la organización

Visión General

El capítulo 4 establece la base estratégica del SGIA. En esencia, responde a una pregunta central: ¿en qué contexto opera la organización y qué necesita gestionar respecto a la IA? Incluye cuatro componentes: 4.1 comprensión del contexto, 4.2 necesidades y expectativas de partes interesadas, 4.3 determinación del alcance y 4.4 sistema de gestión de IA.

Este capítulo es el punto de partida del sistema: sin contexto, no hay alcance sólido; sin alcance, no hay control real. Por ello, antes de definir controles o evidencias, la organización debe entender su entorno, su rol frente a los sistemas de IA y qué factores internos o externos condicionan la gobernanza.

Ejemplo aplicado: antes de definir controles de IA, la organización debe entender su entorno regulatorio y su rol frente al sistema de IA.

Autoevaluación: ¿Puede una organización implementar controles sin haber definido previamente su contexto?

4.1 Comprensión del Contexto

La organización debe determinar los factores internos y externos relevantes para su propósito y su capacidad de lograr los resultados previstos del SGIA. Esto incluye identificar si el cambio climático es un tema pertinente, cuando aplique por contexto, y definir su rol respecto al sistema de IA.

La norma enfatiza que el rol influye en la aplicabilidad de requisitos: quien desarrolla o provee IA tiene obligaciones distintas de quien solo la utiliza. Por tanto, el contexto no es un diagnóstico genérico; es el fundamento que define prioridades, riesgos y el nivel de control esperado.

Ejemplo aplicado: un proveedor de IA tiene obligaciones diferentes a un simple usuario del sistema.

Autoevaluación: ¿Cómo cambia el SGIA si la organización es desarrolladora frente a si es usuaria?

4.2 Necesidades y Expectativas de Partes Interesadas

La organización debe determinar quiénes son las partes interesadas relevantes, qué requisitos tienen, sean legales, contractuales, éticos o de confianza, y cuáles serán abordados por el SGIA.

Este punto asegura que el SGIA no se diseñe en abstracto, sino conectado a obligaciones reales. No todo requisito externo se incorpora automáticamente al alcance, pero sí debe analizarse, decidirse y documentarse qué se aborda y cómo. En IA, es común que reguladores, clientes o usuarios demanden transparencia, explicabilidad o mecanismos de reclamación.

Ejemplo aplicado: un regulador puede exigir transparencia algorítmica, lo que impacta el SGIA.

Autoevaluación: ¿Todos los requisitos de partes interesadas deben incluirse en el alcance del SGIA?

4.3 Determinación del Alcance

El alcance del SGIA debe considerar el contexto (4.1), considerar las partes interesadas (4.2) y estar documentado.

El alcance define los límites del SGIA: qué unidades, procesos y sistemas de IA quedan incluidos. Un alcance claro evita ambigüedades y protege la integridad del sistema en auditoría. Cualquier exclusión debe estar sustentada; de lo contrario, se percibe como una evasión de responsabilidad, especialmente si se trata de sistemas críticos o de alto impacto.

Ejemplo aplicado: una empresa puede incluir solo los sistemas de IA usados en procesos financieros.

Autoevaluación: ¿El alcance puede excluir sistemas críticos sin justificación documentada?

4.4 Sistema de Gestión de IA

La organización debe establecer, implementar, mantener y mejorar continuamente el SGIA, incluyendo los procesos necesarios y sus interacciones. Este requisito conecta directamente con el enfoque PDCA: planificar, ejecutar, verificar y actuar.

Aquí se consolida el paso de definir a operar. No basta con declarar contexto y alcance; el SGIA debe funcionar como sistema vivo, con procesos que se integran: gestión del riesgo, control operacional, auditorías, revisión por la dirección y mejora. La coherencia entre procesos es parte de la evidencia de madurez.

Ejemplo aplicado: el SGIA debe tener procesos definidos para riesgo, auditoría, revisión y mejora.

Autoevaluación: ¿El SGIA es un proyecto temporal o un sistema permanente?

Capítulo 5 – Liderazgo

5.1 Liderazgo y Compromiso

La Alta Dirección debe demostrar liderazgo y compromiso con el SGIA. Esto implica integrar el SGIA en los procesos de negocio, proveer recursos, promover la mejora continua y asegurar el logro de resultados previstos.

La responsabilidad no es delegable completamente. Aunque existan roles especializados, como gobernanza, riesgo o compliance, el compromiso visible de la Alta Dirección es una condición de eficacia: da legitimidad, prioridad y continuidad al sistema. Sin liderazgo, el SGIA tiende a convertirse en un esfuerzo documental sin tracción operativa.

Ejemplo aplicado: el CEO debe aprobar la política de IA.

Autoevaluación: ¿Puede el SGIA funcionar sin compromiso visible de la Alta Dirección?

5.2 Política de IA

La política debe ser apropiada al propósito y al contexto, incluir compromiso con requisitos aplicables, incluir compromiso con mejora continua, y estar documentada y comunicada.

Además, debe servir como marco para establecer objetivos de IA. Una política eficaz traduce intención estratégica en dirección operativa: define principios y límites. En IA,

esto suele abarcar transparencia, responsabilidad, supervisión, tratamiento de riesgos y cumplimiento.

Ejemplo aplicado: la política puede establecer principios de transparencia y responsabilidad.

Autoevaluación: ¿Qué diferencia hay entre política y objetivo?

5.3 Roles, Responsabilidades y Autoridades

La Alta Dirección debe asignar y comunicar responsabilidades para asegurar la conformidad del SGIA y reportar el desempeño del SGIA.

Debe existir claridad organizacional: quién decide, quién ejecuta y quién reporta. En un SGIA, la falta de asignación formal genera riesgos típicos: decisiones no trazables, controles sin dueño, evidencia incompleta y, en el peor caso, gobernanza de nombre sin capacidad real de gestión.

Ejemplo aplicado: un AI Governance Lead puede ser responsable de reportar desempeño.

Autoevaluación: ¿Qué riesgo existe si las responsabilidades no están formalmente asignadas?

Capítulo 6 – Planificación

6.1 Acciones para Riesgos y Oportunidades

La organización debe determinar riesgos y oportunidades, establecer criterios de riesgo y planificar acciones para abordarlos.

El enfoque es basado en riesgo: se planifica para evitar desviaciones en resultados previstos y para capturar oportunidades de mejora. En IA, esto es clave porque el entorno cambia con rapidez, incluyendo datos, regulación y usos. La planificación conecta estrategia con control: convierte incertidumbre en decisiones documentadas.

Ejemplo aplicado: riesgo, sesgo en el modelo; oportunidad, mejora de eficiencia operacional.

Autoevaluación: ¿La norma exige eliminar todos los riesgos?

6.1.2 Evaluación de Riesgos de IA

Debe existir un proceso que identifique riesgos, analice consecuencias y probabilidad, determine niveles de riesgo y priorice su tratamiento.

El proceso debe ser repetible y consistente. Esto evita evaluaciones ad hoc y permite comparar riesgos entre sistemas, procesos o periodos. En IA, la evaluación del riesgo suele requerir un enfoque integral: impacto en usuarios, cumplimiento, reputación y operación.

Ejemplo aplicado: se evalúa el impacto de decisiones automatizadas en usuarios vulnerables.

Autoevaluación: ¿Qué diferencia hay entre análisis y evaluación del riesgo?

6.1.3 Tratamiento de Riesgo de IA

La organización debe seleccionar opciones de tratamiento, comparar controles con el Anexo A, elaborar la SoA y aprobar el riesgo residual.

El tratamiento conecta directamente con controles. Aquí se formaliza la decisión: qué se hará frente al riesgo y con qué medidas. La SoA funciona como evidencia de trazabilidad: muestra qué controles se seleccionan y por qué.

💡 **TIP DE EXAMEN:** Si una pregunta habla de exclusión o inclusión de controles, riesgo residual o justificación documental, piensa primero en 6.1.3 y en la SoA.

Ejemplo aplicado: implementar validación independiente como control mitigador.

Autoevaluación: ¿Puede excluirse un control del Anexo A sin justificación?

6.1.4 Evaluación de Impacto del Sistema de IA

Es un proceso formal para identificar impactos en individuos, grupos y sociedad.

Debe documentarse y alimentar la evaluación de riesgos. Impacto y riesgo no son equivalentes: el impacto describe consecuencias; el riesgo combina consecuencias con probabilidad. En IA, evaluar impacto permite anticipar efectos no deseados, especialmente cuando hay decisiones automatizadas, poblaciones vulnerables o implicaciones de derechos.

Ejemplo aplicado: evaluar si el sistema afecta derechos fundamentales.

Autoevaluación: ¿La evaluación de impacto reemplaza la evaluación de riesgos?

6.2 Objetivos de IA

Los objetivos de IA deben ser coherentes con la política, ser medibles cuando sea posible, ser monitoreados y estar documentados.

Contribuyen al desempeño del SGIA, porque transforman la intención, es decir la política, en metas verificables. Un objetivo sin seguimiento se convierte en declaración; un objetivo con indicadores permite control y mejora.

Ejemplo aplicado: reducir incidentes relacionados con sesgo en 30 % anual.

Autoevaluación: ¿Un objetivo no medible cumple totalmente el requisito?

6.3 Planificación de Cambios

Los cambios en el SGIA deben planificarse, evaluarse en términos de impacto e implementarse de forma controlada.

Esto evita disrupciones no controladas. En IA, cambios pequeños pueden tener efectos amplios, por ejemplo en datos, proveedor o finalidad de uso. Por eso, la planificación de cambios protege la consistencia del sistema y mantiene la trazabilidad.

Ejemplo aplicado: cambio en proveedor de datos requiere nueva evaluación de riesgo.

Autoevaluación: ¿Qué ocurre si un cambio significativo no es planificado formalmente?

Capítulo 7 – Soporte

7.1 Recursos

La organización debe proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar el SGIA. Esto incluye recursos humanos, tecnológicos y financieros. La lógica es directa: un sistema de gestión no funciona por intención, sino por capacidad instalada. Sin recursos, los requisitos se vuelven declarativos.

Además, el provisionamiento de recursos debe ser coherente con el alcance y el nivel de riesgo asociado a los sistemas de IA gestionados. En la práctica, esto implica asignar tiempo, presupuesto y herramientas para actividades como evaluación de riesgos, control operacional, formación, auditoría interna y mejora.

Ejemplo aplicado: asignar presupuesto para auditoría interna del SGIA.

Autoevaluación: ¿Puede el SGIA operar sin recursos asignados formalmente?

7.2 Competencia

La organización debe determinar las competencias necesarias para el trabajo que afecta el desempeño del SGIA, asegurar formación o experiencia adecuada y mantener evidencia documentada. La competencia es un requisito formal: no basta con tener personal; es necesario demostrar que las personas tienen capacidades pertinentes y verificables.

En IA, la competencia puede abarcar disciplinas diversas: gobernanza, evaluación de riesgos, aspectos legales, ética, privacidad, seguridad, calidad de datos o validación de modelos. En términos de certificación, el punto crítico es la evidencia: si no se puede demostrar competencia con registros, la conformidad queda comprometida.

Ejemplo aplicado: formación en evaluación de impacto para el equipo de IA.

Autoevaluación: ¿La experiencia informal sin evidencia cumple el requisito?

7.3 Toma de Conciencia

Las personas deben conocer la política de IA, su contribución al SGIA y las consecuencias del incumplimiento. La toma de conciencia impacta la eficacia del sistema porque reduce desviaciones operativas y evita que el cumplimiento dependa solo de especialistas.

Este requisito no significa que toda la organización deba dominar la norma; significa que quienes influyen en el SGIA deben entender lo esencial: principios de la política, responsabilidades básicas y efectos de no seguir procesos establecidos. En IA, donde cambios pequeños pueden generar efectos amplios, la conciencia organizacional actúa como una capa preventiva.

Ejemplo aplicado: desarrolladores informados sobre implicaciones éticas del modelo.

Autoevaluación: ¿Puede existir conformidad si el personal desconoce la política?

7.4 Comunicación

Debe determinarse qué comunicar, cuándo, a quién y cómo. Esto incluye comunicación interna y externa. La comunicación es un requisito de control: asegura consistencia, transparencia y trazabilidad, especialmente cuando existen partes interesadas con expectativas relevantes, como reguladores, clientes y usuarios.

No se trata de comunicar más, sino de comunicar mejor: con criterios, responsables, canales y momentos definidos. En IA, la comunicación puede incluir temas como incidentes, cambios significativos, limitaciones del sistema, responsabilidades o requerimientos de uso.

Ejemplo aplicado: comunicar incidentes relevantes a reguladores.

Autoevaluación: ¿La norma exige comunicación externa obligatoria en todos los casos?

7.5 Información Documentada

El SGIA debe incluir la información documentada requerida por la norma y la necesaria para su eficacia. Además, debe controlarse: identificación, versionado, acceso y retención. Es equivalente al control documental en otras normas ISO.

La idea central es la confiabilidad: si los documentos no están controlados, la organización no puede demostrar consistencia, ni asegurar que se trabaja con versiones vigentes. En auditoría, este es un punto crítico: procedimientos, registros y evidencias deben estar disponibles, protegidos y trazables.

Ejemplo aplicado: control de versiones de la evaluación de impacto.

Autoevaluación: ¿Un documento sin control de versiones cumple el requisito?

Capítulo 8 – Operación

Visión General

El Capítulo 8 asegura que lo planificado en el Capítulo 6 se implemente operativamente. Incluye 8.1 planificación y control operacional, 8.2 evaluación de riesgos de IA, 8.3 tratamiento del riesgo de IA y 8.4 evaluación de impacto del sistema de IA. Es la fase Do del ciclo PDCA.

La intención es clara: el SGIA debe bajar a procesos reales. En este capítulo se evidencian controles en funcionamiento, registros de ejecución y mecanismos de supervisión operativa. Sin operación controlada, la planificación se queda en intención.

Ejemplo aplicado: después de planificar el tratamiento del riesgo, la organización debe ejecutar controles en el desarrollo del modelo.

Autoevaluación: ¿Puede existir un SGIA eficaz sin controles operativos implementados?

8.1 Planificación y Control Operacional

La organización debe planificar los procesos necesarios, establecer criterios, controlar procesos conforme a esos criterios e implementar controles definidos en 6.1.3. Este requisito asegura coherencia entre planificación y ejecución.

El matiz importante es el criterio: operar no es ejecutar tareas, sino ejecutarlas bajo condiciones definidas. En IA, esto puede implicar criterios de validación, condiciones de despliegue, criterios de monitoreo o límites de uso. Operación controlada significa que el sistema se gestiona con reglas claras, no por improvisación.

Ejemplo aplicado: definir los criterios de validación obligatoria antes del despliegue de un modelo.

Autoevaluación: ¿Qué diferencia existe entre planificación (Cap. 6) y control operacional (Cap. 8)?

Integración de Controles en la Operación

Los controles seleccionados deben integrarse en procesos reales, ser monitoreados y evaluarse en términos de eficacia. La operación incluye el ciclo de vida del sistema de IA.

Este punto es clave: un control definido no equivale a un control implementado. Para considerarse operativo, debe existir evidencia de su aplicación, como registros, resultados y revisiones. Además, la eficacia debe verificarse: un control puede existir y aun así ser insuficiente para reducir el riesgo como se esperaba.

Ejemplo aplicado: control, revisión independiente del modelo antes de producción.

Autoevaluación: ¿Un control definido pero no implementado genera conformidad?

Gestión de Cambios Operacionales

La organización debe controlar cambios planificados, revisar consecuencias de cambios no previstos y mitigar efectos adversos. El cambio puede ser técnico u organizacional.

En IA, la gestión de cambios es especialmente sensible: modificaciones en datos, objetivos, contexto de uso o dependencias pueden alterar el comportamiento del sistema. Por eso, el control de cambios protege la estabilidad del SGIA y evita que el riesgo aumente silenciosamente por cambios no evaluados.

Ejemplo aplicado: cambio en algoritmo requiere reevaluación de impacto.

Autoevaluación: ¿Un cambio menor requiere evaluación formal?

Control de Procesos Externos

Debe asegurarse el control de proveedores, servicios externos y componentes de terceros. El SGIA mantiene la responsabilidad organizacional.

La idea central es simple: externalizar no equivale a transferir responsabilidad. Una organización puede depender de terceros, como nube, datos o modelos, pero debe definir criterios, controles y mecanismos de supervisión para asegurar que la operación se mantiene conforme al SGIA. Esto conecta con la gestión de partes interesadas y requisitos contractuales.

Ejemplo aplicado: el proveedor cloud que aloja el modelo debe cumplir criterios de seguridad definidos.

Autoevaluación: ¿La responsabilidad del SGIA se transfiere al proveedor?

8.2 Evaluación de Riesgos en Operación

La evaluación de riesgos debe realizarse a intervalos planificados y cuando existan cambios significativos. Debe conservarse información documentada.

Esto confirma que la evaluación del riesgo no es un ejercicio de arranque. En IA, el riesgo puede cambiar por nuevas fuentes de datos, nuevas funcionalidades, ampliación de usuarios o cambios regulatorios. Por eso, el SGIA exige periodicidad y trazabilidad: evidenciar cuándo se evaluó, con qué método y qué se decidió.

Ejemplo aplicado: un nuevo tipo de datos ingresado al sistema activa una reevaluación.

Autoevaluación: ¿La evaluación de riesgos es una actividad única o recurrente?

Reevaluación ante Cambios

Cambios significativos pueden incluir nuevos usos del sistema, nuevos datos o nuevas regulaciones. En estos casos, la evaluación debe actualizarse.

Un cambio puede ser significativo aunque no sea técnicamente complejo. Lo importante es el efecto potencial en riesgos e impactos. Por ello, la organización debe definir criterios internos para reconocer significatividad y evitar decisiones arbitrarias.

Ejemplo aplicado: un sistema inicialmente interno se ofrece ahora a clientes externos.

Autoevaluación: ¿Qué constituye un cambio significativo?

8.3 Implementación del Tratamiento del Riesgo

La organización debe ejecutar el plan de tratamiento, verificar su eficacia y actualizar el plan si es ineficaz. La eficacia es requisito explícito.

La implementación se evalúa por resultados, no por intención. Un control puede implementarse correctamente y aun así no reducir el riesgo lo suficiente. En ese caso, el SGIA exige ajuste: reforzar controles, cambiar estrategia o redefinir criterios. Este enfoque protege la eficacia real del sistema.

Ejemplo aplicado: si el control de sesgo no reduce desviaciones, debe ajustarse.

Autoevaluación: ¿Implementar un control garantiza automáticamente su eficacia?

Documentación del Tratamiento

Debe conservarse evidencia de resultados del tratamiento y verificación de eficacia. La trazabilidad es esencial.

La evidencia demuestra que el tratamiento se ejecutó, que se midió su efecto y que se tomaron decisiones con base en resultados. Sin registros, la organización no puede demostrar conformidad ni aprendizaje. Además, la documentación habilita continuidad: permite que el sistema se sostenga aun cuando cambien responsables o equipos.

Ejemplo aplicado: registro formal de validaciones posteriores al despliegue.

Autoevaluación: ¿La ausencia de evidencia documental puede generar no conformidad?

8.4 Evaluación de Impacto en Operación

Debe realizarse a intervalos planificados y ante cambios significativos. Los resultados deben documentarse.

Este requisito asegura que la evaluación de impacto no quede restringida a etapas iniciales. En operación, el sistema puede interactuar con realidades nuevas: cambios en usuarios, contextos, datos o finalidades. Por ello, mantener la evaluación de impacto actualizada es una forma de prevenir daños y sostener la confianza.

Ejemplo aplicado: impacto reevaluado tras ampliar funcionalidad de IA.

Autoevaluación: ¿La evaluación de impacto es opcional en fase operativa?

Relación entre Riesgo e Impacto

La evaluación de impacto alimenta la evaluación de riesgos.

Impacto describe consecuencias. Riesgo combina probabilidad y consecuencia.

Ambos procesos están conectados. Un impacto alto puede elevar el nivel de riesgo, incluso si la probabilidad es moderada. Esta relación es clave para priorizar tratamiento y justificar controles, especialmente en casos donde hay potencial de afectación a derechos o a grupos sensibles.

Ejemplo aplicado: impacto alto en derechos fundamentales aumenta el nivel de riesgo.

Autoevaluación: ¿Impacto y riesgo son conceptos equivalentes?

Ciclo de Vida del Sistema de IA

La operación cubre desarrollo, despliegue, uso, mantenimiento y retiro. El SGIA debe acompañar todo el ciclo.

La razón es sencilla: el riesgo no termina cuando el sistema entra en producción. Al contrario, muchos riesgos emergen o se evidencian en uso real, como desviaciones, cambios en datos o cambios en comportamiento. Además, el retiro ordenado también requiere control: gestión documental, desactivación segura y cierre de dependencias.

Ejemplo aplicado: el desmantelamiento del sistema requiere control documental.

Autoevaluación: ¿El SGIA termina cuando el sistema entra en producción?

Monitoreo Operativo Continuo

Incluye supervisión del desempeño, detección de desviaciones y gestión de incidentes. Permite actuar preventivamente.

El monitoreo operativo es un mecanismo de control diario o continuo: identifica señales tempranas antes de que se conviertan en fallos mayores. En IA, estas señales pueden ser cambios en tasas de error, resultados inesperados, degradación de desempeño o incidentes relacionados con uso indebido.

Ejemplo aplicado: el sistema detecta un aumento inusual de errores.

Autoevaluación: ¿Qué diferencia hay entre monitoreo (Cap. 8) y evaluación del desempeño (Cap. 9)?

Integración con Controles del Anexo A

Los controles implementados en operación pueden derivar de A.6, sobre ciclo de vida; A.7, sobre datos; A.8, sobre información a partes interesadas; y A.9, sobre uso responsable.

El Anexo A es referencia, no obligatorio en su totalidad. Lo esencial es la trazabilidad: controles seleccionados según el riesgo, implementados en operación y verificados en eficacia.

Ejemplo aplicado: el control A.7.4 asegura la calidad de datos en operación.

Autoevaluación: ¿Es obligatorio aplicar todos los controles del Anexo A?

Cierre del Capítulo 8

El Capítulo 8 garantiza que lo planificado se ejecuta, los riesgos se gestionan dinámicamente, los impactos se revisan y la evidencia se conserva.

Es el corazón operativo del SGIA porque traduce la gobernanza en prácticas reales. Si el Capítulo 6 define qué se hará, el Capítulo 8 evidencia que efectivamente se hizo, con controles en funcionamiento y registros disponibles.

Autoevaluación: ¿Podrías explicar cómo el Capítulo 6 y el Capítulo 8 se complementan?

Capítulo 9 – Evaluación del desempeño

Visión General

El Capítulo 9 corresponde a la fase Check del PDCA. Incluye 9.1 monitoreo y medición, 9.2 auditoría interna y 9.3 revisión por la dirección. Evalúa la eficacia del SGIA.

La diferencia clave respecto al Capítulo 8 es la intención: en operación se ejecuta y monitorea el sistema; en evaluación se revisa formalmente su eficacia y conformidad, con enfoque de control y mejora. El Capítulo 9 produce evidencia para decisiones de la Alta Dirección y para acciones de mejora.

Autoevaluación: ¿Por qué la auditoría no pertenece al Capítulo 8?

9.1 Monitoreo y Medición

Debe determinarse qué monitorear, métodos, cuándo y cómo evaluar resultados. Debe existir evidencia documentada.

Este requisito formaliza el sistema de indicadores: no se mide por intuición. Se definen métricas, frecuencia y responsables. El valor no está solo en medir, sino en evaluar resultados y usarlos para decisiones. Sin evidencia, no hay demostración de control.

Ejemplo aplicado: indicador, número de incidentes relacionados con IA.

Autoevaluación: ¿Monitorear sin analizar resultados cumple el requisito?

Evaluación de Eficacia del SGIA

La organización debe evaluar desempeño y eficacia del sistema, no solo el desempeño técnico del modelo.

Esto es crucial: el SGIA es un marco organizacional. Su eficacia se observa en si los procesos funcionan, si los controles reducen riesgos, si se cumple la política y si existe mejora continua. Un modelo puede rendir bien técnicamente y, aun así, el SGIA ser ineficaz si no hay control documental, roles claros o gestión de cambios.

Ejemplo aplicado: evaluar si los controles reducen los riesgos previstos.

Autoevaluación: ¿El desempeño del modelo es igual al desempeño del SGIA?

9.2 Auditoría Interna

Debe realizarse a intervalos planificados, evaluar conformidad y evaluar implementación eficaz. Debe existir un programa de auditoría.

La auditoría interna es un mecanismo de verificación independiente dentro del sistema: confirma si el SGIA cumple requisitos y si se aplica de manera efectiva. No se orienta a buscar culpables, sino a evaluar el sistema, identificar brechas y alimentar la mejora.

Ejemplo aplicado: auditoría anual del SGIA.

Autoevaluación: ¿La auditoría interna evalúa personas o evalúa el sistema?

Programa de Auditoría

Debe definir frecuencia, métodos, responsabilidades y reporte. Debe considerarse la importancia de procesos y resultados previos.

Esto introduce el principio de priorización: no todo se audita igual. Procesos críticos o con historial de no conformidades pueden requerir mayor frecuencia o profundidad. El programa de auditoría debe ser planificado, documentado y ejecutado, generando evidencia de revisión sistemática.

Ejemplo aplicado: proceso crítico auditado con mayor frecuencia.

Autoevaluación: ¿Todos los procesos deben auditarse con la misma frecuencia?

9.3 Revisión por la Dirección

La Alta Dirección debe revisar el SGIA para asegurar su idoneidad, adecuación y eficacia. Es un requisito formal.

La revisión por la dirección garantiza gobernanza real: permite evaluar desempeño, cambios en contexto, riesgos emergentes y oportunidades de mejora. Además, produce decisiones: ajustes en política, objetivos, recursos o prioridades. En certificación, se espera evidencia de que esta revisión ocurre y de que genera salidas documentadas.

Ejemplo aplicado: revisión anual del desempeño del SGIA.

Autoevaluación: ¿Puede delegarse completamente la revisión por la dirección?

Entradas y Salidas de la Revisión

Las entradas incluyen resultados de auditoría, no conformidades, cambios en contexto y oportunidades de mejora. Las salidas incluyen decisiones y acciones.

Este requisito enfatiza trazabilidad: la revisión debe basarse en información sólida, es decir, entradas, y producir consecuencias verificables, es decir, salidas. No es una reunión informativa; es un mecanismo de dirección del sistema. Las salidas deben documentarse para demostrar que se tomaron decisiones y se asignaron acciones.

Ejemplo aplicado: decidir actualizar la política de IA.

Autoevaluación: ¿La revisión debe producir decisiones documentadas?

Capítulo 10 – Mejora

10.1 Mejora Continua

La organización debe mejorar la idoneidad, adecuación y eficacia del SGIA. Es un requisito permanente.

La mejora continua no implica innovación tecnológica constante; implica fortalecer el sistema de gestión: procesos más consistentes, controles más eficaces, decisiones mejor informadas y reducción sostenida del riesgo residual. En IA, esta mejora es crítica por la velocidad de cambio en datos, contextos y expectativas regulatorias.

Ejemplo aplicado: optimizar el proceso de evaluación de impacto.

Autoevaluación: ¿La mejora continua implica siempre cambio tecnológico?

10.2 No Conformidad y Acción Correctiva

Cuando ocurre una no conformidad, debe corregirse, analizar su causa, implementar acción correctiva, verificar eficacia y documentarse.

Este punto sintetiza la madurez del sistema: no basta con corregir, se requiere aprendizaje organizacional. El análisis de causa evita recurrencia; la verificación de eficacia demuestra que la solución funcionó. La documentación, además, crea memoria institucional y evidencia para auditoría.

Ejemplo aplicado: una auditoría detecta ausencia de evidencia de competencia.

Autoevaluación: ¿Corregir sin analizar la causa cumple el requisito?

Cierre del Módulo 2 – Estructura Completa del SGIA (Capítulos 4–10)

El Módulo 2 ha desarrollado de manera estructurada los requisitos del SGIA conforme a ISO/IEC 42001, cubriendo la arquitectura completa: Capítulo 4, contexto de la organización; Capítulo 5, liderazgo; Capítulo 6, planificación, incluyendo riesgos, oportunidades y objetivos; Capítulo 7, soporte, incluyendo recursos, competencia e información documentada; Capítulo 8, operación, con ejecución y control operacional; Capítulo 9, evaluación del desempeño; y Capítulo 10, mejora.

Estos capítulos conforman el ciclo integral PDCA: Plan (4–6), Do (7–8), Check (9), Act (10). El Dominio B evalúa tu capacidad para ubicar requisitos en su capítulo, comprender la relación lógica entre planificación, operación, evaluación y mejora, y diferenciar responsabilidades de liderazgo, ejecución y control. Con esta visión sistémica, la norma se entiende como un sistema dinámico de gobernanza de IA, no como cláusulas aisladas.

Ejemplo integrador: si la organización detecta un nuevo riesgo regulatorio, como contexto del Capítulo 4, debe planificar acciones en el Capítulo 6, implementar controles en el Capítulo 8, medir su eficacia en el Capítulo 9 y ajustar el sistema si es necesario en el Capítulo 10.

Autoevaluación: ¿Podrías explicar de memoria cómo se conectan los capítulos 4 al 10 dentro del ciclo PDCA del SGIA?

MÓDULO 3 – SoA Y ANEXOS A/B/C/D

Introducción al Dominio C

El Dominio C evalúa la comprensión de la Declaración de Aplicabilidad (SoA), el propósito del Anexo A, la relación entre controles y riesgos, y la función orientativa de los anexos adicionales. En el examen Foundation, es frecuente que se evalúe la diferencia entre requisitos, ubicados en los Capítulos 4–10; controles de referencia, ubicados en el Anexo A; y orientación, ubicada en el Anexo B.

Este dominio es especialmente sensible porque exige criterio: no basta con reconocer términos, hay que entender su jerarquía normativa. Dicho de otro modo, el candidato debe saber qué obliga, qué orienta y qué se selecciona en función del riesgo. Esa claridad evita errores típicos en examen, como asumir que todo control del Anexo A es obligatorio por defecto.

Ejemplo aplicado: si una organización implementa un control, debe poder demostrar por qué fue seleccionado y cómo se vincula con riesgos identificados.

Autoevaluación: ¿El Anexo A contiene requisitos obligatorios o controles de referencia?

Declaración de Aplicabilidad (SoA)

¿Qué es la Declaración de Aplicabilidad (SoA)?

La **SoA** es un documento obligatorio del SGIA que enumera los controles necesarios, justifica la inclusión o exclusión de controles y se basa en la evaluación y el tratamiento del riesgo. No es un checklist genérico; es un documento contextualizado que refleja decisiones organizacionales.

La SoA tiene un valor probatorio: demuestra que la organización analizó su contexto, priorizó riesgos y eligió controles con lógica y trazabilidad. Por eso, una SoA sólida no se limita a marcar casillas; explica el razonamiento que sostiene la aplicabilidad. En términos de examen, lo clave no es memorizar un formato, sino comprender su función: ser el puente documentado entre riesgos y controles.

Ejemplo aplicado: si un control del Anexo A no aplica porque la organización no desarrolla modelos, debe justificarse formalmente.

Autoevaluación: ¿Puede excluirse un control sin documentar la justificación?

Relación entre Riesgo y SoA

Secuencia lógica: evaluación de riesgos → tratamiento del riesgo → selección de controles → SoA. La SoA es el puente entre el análisis del riesgo y los controles implementados. En otras palabras, la SoA documenta el por qué y el qué del tratamiento, dejando evidencia de la coherencia interna del SGIA.

Este punto suele evaluarse en el examen mediante preguntas de relación causal: si no existe evaluación de riesgos, la SoA pierde fundamento; si no hay tratamiento, la selección de controles es arbitraria. Por tanto, la SoA se entiende como resultado, no como punto de partida.

Ejemplo aplicado: riesgo, uso indebido de datos; control seleccionado, validación de calidad y trazabilidad de datos; registrado en la SoA.

Autoevaluación: ¿Puede existir una SoA sin evaluación de riesgos previa?

Contenido Típico de una SoA

La SoA suele incluir lista de controles del Anexo A, estado (aplicable / no aplicable), justificación, y referencia a la implementación, por ejemplo, procedimiento interno o evidencia. Además, debe mantenerse actualizada para reflejar cambios en contexto, riesgos o controles.

Lo esencial no es la cantidad de controles listados, sino la trazabilidad: cada aplica/no aplica debe sostenerse en lógica organizacional. En la práctica, la SoA es un documento vivo: si el sistema de IA cambia, si hay nuevos riesgos o si se actualizan controles, la SoA debe reflejarlo. Por eso, se considera una pieza central de control documental del SGIA.

Ejemplo aplicado: control A.7.4 marcado como aplicable, con referencia a un procedimiento interno.

Autoevaluación: ¿La SoA es un documento estático o dinámico?

Errores Comunes en la SoA

Errores frecuentes: copiar todos los controles sin análisis, excluir controles sin justificación, o no actualizar la SoA tras cambios. En el examen, se evalúa la comprensión conceptual, no un formato específico.

El riesgo de estos errores es doble: por un lado, debilitan la coherencia del SGIA; por otro, generan vulnerabilidad en auditoría al evidenciar falta de trazabilidad. Copiar controles

por cobertura puede inflar el sistema sin eficacia real. Excluir controles críticos sin sustento, en cambio, sugiere que la evaluación de riesgos fue incompleta o inconsistente.

⚠️ **ALERTA DE ERROR:** La SoA no es un inventario automático del Anexo A. Es la evidencia documentada de decisiones de control basadas en riesgo.

Ejemplo aplicado: excluir un control de monitoreo sin justificación pese a alto riesgo operativo.

Autoevaluación: ¿Qué implica excluir un control crítico sin sustento documentado?

Anexo A – Controles de referencia

Propósito del Anexo A

El Anexo A proporciona un conjunto de controles de referencia organizados temáticamente. No son automáticamente obligatorios; su aplicabilidad depende del análisis de riesgos. En términos prácticos, el Anexo A funciona como un catálogo de controles: ayuda a la organización a comparar opciones y a justificar decisiones de tratamiento.

Este punto es clave para el examen: la norma exige un sistema de gestión, ubicado en los Capítulos 4–10. El Anexo A ofrece controles posibles, pero la organización debe decidir cuáles son necesarios según su contexto y riesgos. Así, dos organizaciones pueden tener SoA distintas y ambas ser conformes, siempre que exista coherencia documentada.

Ejemplo aplicado: una organización pequeña puede aplicar menos controles que una de alto impacto, siempre que esté justificado.

Autoevaluación: ¿Todos los controles del Anexo A deben implementarse obligatoriamente?

Estructura del Anexo A

El Anexo A incluye controles agrupados en dominios como políticas y gobernanza, ciclo de vida del sistema de IA, gestión de datos, información para partes interesadas y uso responsable de IA. Conceptualmente, se parece a la lógica de anexos de controles en otras normas, como ISO/IEC 27001.

La utilidad de esta estructura es organizativa: permite seleccionar controles por temática, facilitar mapeos internos y mantener consistencia. Además, ayuda a

relacionar riesgos específicos con familias de controles, por ejemplo sesgo con controles de datos y evaluación, o transparencia con controles de información a interesados.

Ejemplo aplicado: controles sobre calidad de datos impactan directamente riesgos de sesgo.

Autoevaluación: ¿El Anexo A sustituye los requisitos de los capítulos 4–10?

Políticas Relacionadas con la IA

El Anexo A incluye controles de referencia orientados a fortalecer las políticas relacionadas con la IA, más allá del requisito obligatorio del Capítulo 5.

Mientras el Capítulo 5 exige la existencia de una Política de IA formal, el Anexo A propone controles que pueden ampliar su contenido, tales como declaración explícita de principios de uso responsable, integración con políticas de seguridad, privacidad o calidad, lineamientos sobre transparencia, supervisión humana y mitigación de sesgos, y compromiso con cumplimiento regulatorio y expectativas éticas.

Distinción clave para el examen: la política es un requisito obligatorio. El contenido detallado sugerido por el Anexo A es un control de referencia, aplicable según contexto y riesgos.

Ejemplo aplicado: una organización incorpora en su política compromisos explícitos sobre explicabilidad algorítmica.

Autoevaluación: ¿El contenido ampliado de la política proviene del capítulo obligatorio o del Anexo A?

Organización Interna y Gobernanza

Este grupo de controles refuerza la dimensión organizacional del SGIA. Se relaciona directamente con el Capítulo 5.3, sobre roles, responsabilidades y autoridades, pero propone mecanismos más estructurados, tales como establecimiento de estructuras formales de gobernanza de IA, creación de comités de supervisión o funciones independientes de validación, definición de líneas de reporte para incidentes relacionados con IA y separación de funciones críticas, por ejemplo desarrollo y validación.

El punto clave es que el Anexo A no obliga a crear una estructura específica, pero sí sugiere controles para fortalecer la gobernanza cuando el nivel de riesgo lo justifique.

Ejemplo aplicado: una organización crea un Comité de Gobernanza de IA para supervisar decisiones críticas.

Autoevaluación: ¿La creación de un comité de IA es un requisito obligatorio o un control de referencia?

Recursos para Sistemas de IA

Relacionado con el Capítulo 7.1, este grupo de controles enfatiza que los sistemas de IA requieren capacidades específicas para sostener su gobernanza. Los controles pueden abordar disponibilidad de infraestructura técnica adecuada, recursos para validación independiente, capacidades para monitoreo continuo y herramientas para trazabilidad y auditoría.

Mientras el capítulo exige proporcionar recursos, el Anexo A detalla qué tipos de recursos son particularmente relevantes en entornos de IA.

En Foundation es importante distinguir: el requisito es proveer recursos. El detalle sobre qué recursos son críticos puede derivar del Anexo A.

Ejemplo aplicado: asignar herramientas específicas para monitorear sesgos en producción.

Autoevaluación: ¿La falta de herramientas de monitoreo podría impactar la eficacia del SGIA?

Evaluación de Impactos – Controles Complementarios

Aunque la evaluación de impacto es un requisito normativo, en los Capítulos 6 y 8, el Anexo A incluye controles que pueden fortalecer la forma en que dicha evaluación se realiza y mantiene. Estos pueden incluir metodologías estructuradas para identificar impactos en individuos y grupos, criterios específicos para evaluar impactos en poblaciones vulnerables y procedimientos de revisión periódica de impactos durante la operación.

Aquí es fundamental no confundir niveles normativos: la evaluación de impacto es obligatoria. La metodología específica puede apoyarse en controles de referencia del Anexo A.

Ejemplo aplicado: implementar una matriz estandarizada para evaluar impactos sociales del sistema.

Autoevaluación: ¿Impacto y riesgo son equivalentes dentro del SGIA?

Controles del Ciclo de Vida de IA

Incluyen controles relacionados con diseño, desarrollo, validación, despliegue y retiro. Su propósito es reforzar la gestión integral del sistema a lo largo del ciclo de vida, evitando que la gobernanza se limite a una fase, por ejemplo solo desarrollo.

La lógica es consistente con el SGIA: si el riesgo cambia con el tiempo, el control también debe acompañar el cambio. Por ello, estos controles suelen asociarse a prácticas de validación previa al despliegue, control de cambios, monitoreo en operación y procedimientos de retiro o desmantelamiento.

Ejemplo aplicado: control que exige pruebas antes del despliegue.

Autoevaluación: ¿El ciclo de vida termina en la fase de desarrollo?

Controles sobre Datos

Controles relacionados con calidad, integridad, procedencia y protección. Son críticos para la confiabilidad del sistema de IA, ya que los datos influyen directamente en resultados, sesgos, consistencia y explicabilidad.

En el SGIA, los datos no se tratan como insumo neutral: su gestión es una fuente clave de riesgo. Por eso, controles de datos suelen enfocarse en validación, trazabilidad, criterios de aceptación, manejo de cambios y protección. Una organización puede tener un modelo técnicamente sólido, pero si los datos son deficientes o no trazables, la gobernanza pierde control.

Ejemplo aplicado: control que exige validación de datos de entrenamiento.

Autoevaluación: ¿Por qué los datos son críticos en el SGIA?

Información a Partes Interesadas

Incluye controles relacionados con transparencia, comunicación e información relevante. Conecta con principios de uso responsable y con expectativas de partes interesadas, como usuarios, clientes y reguladores.

Este conjunto de controles ayuda a gestionar riesgos de confianza, reputación y cumplimiento, especialmente cuando la IA influye en decisiones relevantes. Informar adecuadamente no significa revelar información confidencial, sino asegurar que las partes interesadas reciban información pertinente para comprender el uso del sistema y sus implicaciones.

Ejemplo aplicado: informar a usuarios que interactúan con un sistema automatizado.

Autoevaluación: ¿La transparencia puede mitigar riesgos reputacionales?

Uso Responsable de IA

Controles orientados a mitigar sesgo, evitar impactos negativos y asegurar supervisión humana cuando corresponda. Refuerzan principios éticos y regulatorios, y suelen ser especialmente relevantes en decisiones de alto impacto.

Un punto importante: la supervisión humana no siempre es obligatoria; depende del contexto, el nivel de riesgo y la criticidad. Sin embargo, cuando se aplica, debe ser real y efectiva, no un sello formal. En el examen, esta distinción suele aparecer en preguntas sobre aplicabilidad y proporcionalidad de controles.

Ejemplo aplicado: revisión humana obligatoria para decisiones críticas.

Autoevaluación: ¿La supervisión humana es siempre obligatoria?

Relaciones con Terceros y Clientes

Este grupo conecta con Capítulos 4, 7 y 8. Los controles pueden abordar evaluación de proveedores de componentes de IA, inclusión de cláusulas contractuales específicas sobre IA, mecanismos de supervisión de servicios externalizados y comunicación clara con clientes sobre uso de IA.

Un principio esencial del SGIA es que externalizar no transfiere responsabilidad. La organización mantiene la obligación de gobernar el uso del sistema, incluso cuando depende de terceros.

Ejemplo aplicado: exigir a un proveedor cloud controles de seguridad alineados con el SGIA.

Autoevaluación: ¿La organización puede transferir completamente la responsabilidad del SGIA a un proveedor?

Integración Transversal del Anexo A

El Anexo A no debe interpretarse como bloques aislados de controles técnicos. Su estructura abarca dimensiones estratégicas, organizativas y operativas: políticas, gobernanza interna, recursos, evaluación de impacto, ciclo de vida, datos, transparencia, uso responsable y relaciones externas.

Todos estos grupos se conectan mediante la lógica del SGIA: riesgo identificado → control seleccionado → justificación en SoA → implementación y verificación.

En el examen Foundation, la competencia clave no es memorizar controles específicos, sino comprender su función como herramientas de tratamiento del riesgo alineadas con el contexto organizacional.

Autoevaluación: ¿Puedes explicar cómo los controles del Anexo A apoyan, pero no sustituyen, los requisitos de los capítulos 4–10?

Anexo B – Orientación para implementación

Propósito del Anexo B

El Anexo B proporciona orientación para implementar controles del Anexo A. No contiene requisitos adicionales. Es explicativo y no normativo obligatorio.

Su utilidad es práctica: ayuda a interpretar cómo podría aplicarse un control, qué consideraciones pueden ser relevantes y qué enfoques suelen utilizarse. En certificación, el Anexo B no se audita como requisito; se utiliza como referencia para fortalecer la implementación. En examen Foundation, suele evaluarse precisamente esta diferencia: orientación versus obligatoriedad.

Ejemplo aplicado: describe cómo podría aplicarse un control de validación.

Autoevaluación: ¿El incumplimiento del Anexo B genera no conformidad directa?

Diferencia entre Requisito y Orientación

Capítulos 4–10 corresponden a requisitos obligatorios.

Anexo A corresponde a controles de referencia.

Anexo B corresponde a orientación explicativa.

Esta distinción es crítica para el examen. Confundirla lleva a conclusiones incorrectas, como pensar que implementar el SGIA equivale a aplicar todos los controles del Anexo A o que el Anexo B impone obligaciones adicionales. Lo cierto es que la obligatoriedad recae en los requisitos de los capítulos; los anexos apoyan y guían decisiones basadas en riesgo.

💡 **TIP DE EXAMEN:** Ante cualquier duda, pregunta: ¿esto obliga, orienta o sirve como referencia? Esa jerarquía resuelve gran parte de las preguntas del Dominio C.

Ejemplo aplicado: no implementar un requisito del Capítulo 6 genera no conformidad; no seguir una sugerencia del Anexo B no necesariamente.

Autoevaluación: ¿Puede confundirse el Anexo B con un requisito obligatorio?

Anexo B – Orientaciones para la Implementación de los Controles

El Anexo B proporciona guía práctica para implementar los 39 controles del Anexo A. Su carácter es explícitamente orientativo, no normativo obligatorio. Esto significa que la organización no está obligada a justificar en la SoA la adopción literal de esta guía; puede adaptarla, ampliarla o definir su propio enfoque, siempre alineado con su tratamiento del riesgo, conforme a la Cláusula 6.1.3.

El Anexo B desarrolla orientaciones en ámbitos como políticas de IA, incluyendo alineación, revisión y coherencia con otras políticas; organización interna, incluyendo roles, reporte de preocupaciones y gobernanza; recursos, incluyendo datos, herramientas, infraestructura y competencias; evaluación de impactos, con proceso sistemático y documentación; ciclo de vida completo del sistema de IA; gestión de datos, incluyendo calidad, procedencia y preparación; información a partes interesadas; uso responsable y supervisión humana significativa; y relaciones con terceros y clientes.

Principios transversales destacados incluyen enfoque basado en riesgos, trazabilidad, mejora continua, transparencia y supervisión humana.

Distinción clave para el examen: Capítulos 4–10, requisitos obligatorios; Anexo A, controles de referencia; Anexo B, guía de implementación adaptable.

Autoevaluación: ¿El incumplimiento literal de una recomendación del Anexo B genera automáticamente una no conformidad?

Anexos C y D

Anexo C – Relación con Otros Marcos

El Anexo C describe la relación entre ISO/IEC 42001 y otros marcos relevantes. Facilita integración y alineación normativa, sin introducir requisitos nuevos.

Este anexo es útil para organizaciones que deben demostrar coherencia con otros estándares o marcos regulatorios: ayuda a mapear conceptos, controles o enfoques. En Foundation, suele evaluarse su carácter: aporta contexto y alineación, pero no impone obligaciones adicionales.

Ejemplo aplicado: mapeo entre controles de IA y marcos regulatorios emergentes.

Autoevaluación: ¿El Anexo C es obligatorio para certificación?

Anexo D – Consideraciones Sectoriales

El Anexo D proporciona ejemplos y contexto adicional para orientar la interpretación en sectores específicos. No añade requisitos ni modifica los capítulos principales.

Su valor es interpretativo: muestra cómo ciertos riesgos o expectativas pueden variar por industria, por ejemplo, salud, finanzas o sector público. En el examen, conviene recordar que su función es guiar, no obligar. Dicho de otro modo, ayuda a pensar, no a cumplir.

Ejemplo aplicado: consideraciones especiales en el sector salud.

Autoevaluación: ¿El Anexo D modifica los requisitos de los capítulos principales?

Relación Integral: Riesgo – Control – SoA – Anexos

Secuencia completa: Capítulo 6, identificación y evaluación de riesgos; Anexo A, controles de referencia; SoA, decisión documentada; Anexo B, orientación de implementación.

Esta cadena lógica es evaluable en el examen porque demuestra comprensión sistémica. La clave es la trazabilidad: del riesgo a la decisión de control, en la SoA, y de la decisión a la implementación, con apoyo del Anexo B. Los anexos C y D añaden contexto y alineación, pero no alteran la estructura normativa.

Ejemplo aplicado: riesgo alto → control A.7.x → registrado en SoA → implementado con guía del Anexo B.

Autoevaluación: ¿Puedes explicar esta secuencia sin apoyo visual?

Preguntas Tipo Examen – Dominio C

En el examen Foundation pueden preguntarse qué documento justifica la exclusión de controles, si el Anexo A es obligatorio en su totalidad, si el Anexo B contiene requisitos o si la SoA debe actualizarse tras cambios.

La preparación implica comprensión conceptual clara: jerarquía normativa, trazabilidad y diferencia entre requisito, control de referencia y orientación. En este dominio, la confusión más común es asumir obligatoriedad donde solo hay guía.

Autoevaluación: ¿Te sentirías cómodo respondiendo preguntas comparativas entre Anexo A y Anexo B?

Cierre del Módulo 3

El Módulo 3 ha desarrollado el rol estratégico de la SoA, la estructura y propósito del Anexo A, la función orientativa del Anexo B y el contexto adicional de los Anexos C y D. El Dominio C evalúa la capacidad de diferenciar con precisión requisitos, controles y orientación.

La idea final es simple, pero decisiva: la norma exige un sistema, en los Capítulos 4–10, y la SoA evidencia cómo se seleccionan controles en función del riesgo, con apoyo de anexos que orientan y contextualizan. Con esa claridad, se responde con seguridad tanto en examen como en aplicación profesional.

Autoevaluación: ¿Puedes explicar por qué la SoA es un elemento central del SGIA?

MÓDULO 4 – Roles, Partes Interesadas y Aplicabilidad

Introducción al Dominio D

El Dominio D se centra en comprender quién es responsable dentro del SGIA y a quién impacta el sistema de IA. ISO/IEC 42001 enfatiza que la gestión de la IA no es únicamente técnica: es organizacional, estratégica y, sobre todo, gobernable mediante procesos, responsabilidades y evidencia.

En el examen Foundation, este dominio suele aparecer mediante preguntas situacionales conceptuales: incidentes, decisiones automatizadas, responsabilidades de la Alta Dirección y límites del rol técnico. Por ello, este dominio conecta principalmente con el Capítulo 4, sobre contexto y partes interesadas, y el Capítulo 5, sobre liderazgo y responsabilidades.

La idea clave es directa: aunque existan equipos técnicos altamente competentes, el SGIA exige responsabilidad organizacional explícita y trazable.

Ejemplo aplicado: si ocurre un incidente de IA, la responsabilidad recae en la organización, no únicamente en el equipo técnico.

Autoevaluación: ¿El SGIA es responsabilidad exclusiva del equipo de desarrollo?

Rol de la Organización frente al Sistema de IA

La norma exige que la organización determine su rol respecto al sistema de IA. Puede actuar como desarrolladora, proveedora, integradora, usuaria u operadora.

El rol influye en los requisitos aplicables y, en particular, en el nivel de control esperado sobre el ciclo de vida del sistema. Sin embargo, el punto decisivo es este: el rol no elimina la responsabilidad; solo define su alcance. Incluso cuando el sistema proviene de terceros, la organización sigue siendo responsable de gobernar su uso conforme al SGIA, incluyendo el tratamiento de riesgos asociados a su contexto.

Ejemplo aplicado: una empresa que solo utiliza un sistema de IA de terceros sigue siendo responsable de su uso conforme al SGIA.

Autoevaluación: ¿El rol organizacional modifica la obligación de implementar el SGIA?

Diferencias entre Desarrollador y Usuario

Desarrollador: diseña y entrena modelos, y controla la arquitectura técnica. *Usuario:* implementa el sistema o utiliza sus resultados, y puede no controlar el diseño técnico.

Ambos deben gestionar riesgos asociados a su rol. El desarrollador asume responsabilidades directas sobre el diseño, la validación y el control del ciclo de vida. El usuario, en cambio, debe gobernar el uso: criterios de aplicación, supervisión, límites operativos, monitoreo de resultados y gestión de impactos.

En el examen, esta distinción suele evaluarse para evitar un error típico: creer que el usuario queda libre por no haber desarrollado el modelo. Lo cierto es que el riesgo se manifiesta en el uso real y, por tanto, debe gestionarse desde la operación.

Ejemplo aplicado: un banco que usa un modelo externo debe gestionar riesgos de decisiones automatizadas.

Autoevaluación: ¿Puede un usuario final desentenderse del riesgo porque no desarrolló el modelo?

Responsabilidad de la Alta Dirección

La Alta Dirección debe demostrar liderazgo y compromiso, integrar el SGIA en procesos estratégicos, proveer recursos y asignar responsabilidades.

No puede delegar completamente su responsabilidad. La norma exige que la Alta Dirección no solo apruebe documentos, sino que sostenga el sistema: priorice, supervise y revise resultados. En términos prácticos, la gobernanza de IA debe tener patrocinio real; de lo contrario, el SGIA queda como iniciativa de cumplimiento sin capacidad de influir decisiones.

Esta responsabilidad se evidencia mediante revisiones periódicas, decisiones documentadas y asignación efectiva de recursos.

Ejemplo aplicado: el comité ejecutivo revisa anualmente el desempeño del SGIA.

Autoevaluación: ¿Puede la Alta Dirección limitarse a aprobar la política sin supervisión posterior?

Asignación de Roles y Autoridades

La organización debe definir responsabilidades claras, asignar autoridades y comunicar funciones. La claridad organizacional reduce ambigüedades en la gestión de IA: establece quién decide, quién ejecuta, quién valida y quién reporta.

Cuando las responsabilidades no están documentadas, aparecen fallos previsibles: decisiones no trazables, controles sin dueño, evidencia dispersa y acciones correctivas que se repiten sin resolver causas. En IA, donde los riesgos pueden ser multidimensionales, esta claridad evita vacíos entre áreas, como técnica, legal, negocio y cumplimiento.

Ejemplo aplicado: nombrar formalmente a una persona responsable de gobernanza de IA.

Autoevaluación: ¿Qué riesgo surge si las responsabilidades no están documentadas?

Competencia y Responsabilidad

Las personas que desempeñan funciones dentro del SGIA deben ser competentes. La competencia implica educación, formación, experiencia y evidencia documentada. No basta con experiencia informal: en un sistema de gestión, lo que no puede demostrarse con registros suele considerarse insuficiente.

La competencia no es solo técnica. Puede incluir comprensión de riesgo, gestión documental, evaluación de impacto, controles operativos, comunicación con partes interesadas y cumplimiento. El objetivo es asegurar que quienes toman decisiones o ejecutan controles lo hagan con criterios consistentes y verificables.

Ejemplo aplicado: el equipo de validación debe estar capacitado en evaluación de impacto.

Autoevaluación: ¿Puede una organización declarar competencia sin evidencia verificable?

Partes Interesadas

Identificación de Partes Interesadas

Una parte interesada es cualquier persona u organización que puede afectar decisiones relacionadas con IA o verse afectada por dichas decisiones. Debe identificarse formalmente.

Esta identificación es esencial porque define expectativas, obligaciones y riesgos. En IA, las partes interesadas no se limitan a clientes: pueden incluir usuarios indirectos, personas impactadas por decisiones automatizadas, reguladores, empleados, proveedores y socios. La clave es determinar relevancia para el SGIA, evitando tanto la omisión de actores críticos como listas excesivas sin utilidad.

Ejemplo aplicado: usuarios cuyos datos son utilizados por el sistema.

Autoevaluación: ¿Un regulador siempre es una parte interesada relevante?

Requisitos de Partes Interesadas

La organización debe determinar qué requisitos son aplicables y cuáles deben incorporarse al SGIA. No todos los requisitos externos se incorporan automáticamente, pero sí deben evaluarse y gestionarse.

Esto incluye requisitos legales, contractuales y compromisos organizacionales. La clave es la trazabilidad: si se decide incorporar un requisito, debe reflejarse en procesos, controles o documentación; si no se incorpora, debe existir justificación y gestión del riesgo asociado.

Ejemplo aplicado: un contrato puede exigir auditorías adicionales.

Autoevaluación: ¿Todos los requisitos contractuales deben incluirse dentro del alcance del SGIA?

Transparencia y Comunicación

El SGIA puede requerir comunicación con partes interesadas sobre el funcionamiento general del sistema, riesgos relevantes e incidentes. Esto fortalece la confianza y

cumplimiento. Sin embargo, la transparencia no equivale a divulgar detalles técnicos completos: se trata de proporcionar información pertinente, comprensible y adecuada al propósito.

En el examen, suele evaluarse la diferencia entre transparencia y exposición técnica. Una organización puede ser transparente sin revelar propiedad intelectual o detalles sensibles; lo importante es asegurar que las partes interesadas comprendan el uso de IA, sus límites y, cuando aplique, mecanismos de supervisión o reclamación.

Ejemplo aplicado: informar a clientes que ciertas decisiones son asistidas por IA.

Autoevaluación: ¿La norma obliga a divulgar todos los detalles técnicos del modelo?

Aplicabilidad

Aplicabilidad de ISO/IEC 42001

La norma aplica a cualquier organización que desarrolle, proporcione o utilice sistemas de IA. No depende del tamaño o sector. La aplicabilidad está determinada por la relación con la IA y por el contexto organizacional: si existen riesgos e impactos asociados, existe necesidad de gobernanza.

Este punto es importante para evitar una conclusión errónea: solo aplica a grandes empresas. Una microempresa puede estar altamente expuesta si utiliza IA en decisiones sensibles. Por eso, la norma es flexible: permite ajustar alcance y controles de acuerdo con contexto y riesgo.

Ejemplo aplicado: una startup de análisis predictivo y una entidad pública pueden aplicar la norma.

Autoevaluación: ¿Una microempresa está exenta por tamaño?

Relación entre Aplicabilidad y Alcance

Aplicabilidad no equivale a alcance.

Aplicabilidad: si la norma puede aplicarse a la organización.

Alcance: qué parte específica del negocio está cubierta por el SGIA.

Una organización puede aplicar la norma y definir un alcance parcial, siempre que lo justifique y mantenga coherencia con contexto y partes interesadas. La clave es que el alcance no puede usarse para excluir arbitrariamente sistemas críticos o de alto impacto sin sustento.

Ejemplo aplicado: una empresa aplica la norma solo a su unidad de análisis financiero.

Autoevaluación: ¿Puede una organización aplicar la norma parcialmente?

Cierre del Módulo 4 – Dominio D

Este módulo ha desarrollado el rol organizacional frente a la IA, la responsabilidad de la Alta Dirección, la identificación de partes interesadas y la diferencia entre aplicabilidad y alcance.

El examen evaluará tu capacidad para distinguir roles organizacionales, identificar responsabilidades formales y relacionar partes interesadas con requisitos del SGIA. En términos simples, el Dominio D confirma que comprendes que la gobernanza de IA es una responsabilidad organizacional trazable, no una función exclusivamente técnica.

Autoevaluación: ¿Puedes explicar cómo el rol organizacional influye en la implementación del SGIA?

MÓDULO 5 – Interpretación Básica en Escenarios

Introducción al Dominio E

El Dominio E evalúa la capacidad de aplicar conceptos del SGIA en escenarios breves y prácticos. Las preguntas suelen presentar una situación organizacional, una acción o falta de acción y cuatro opciones de respuesta. La clave es identificar con rapidez el concepto normativo central, por ejemplo política, SoA o auditoría interna; el capítulo correspondiente, del 4 al 10; y si se trata de un requisito obligatorio o de un control de referencia.

En el nivel Foundation no se exige análisis complejo; se exige asociación conceptual correcta. Dicho esto, la asociación debe ser precisa: confundir un requisito con un control del Anexo A o ubicar un tema en el capítulo equivocado suele ser suficiente para fallar la pregunta.

Ejemplo aplicado: una empresa no ha definido formalmente su política de IA. ¿A qué capítulo corresponde esta deficiencia?

Autoevaluación: ¿Podrías ubicar rápidamente un problema en su capítulo correspondiente?

Escenario 1 – Falta de Política Formal

Situación: la organización utiliza sistemas de IA, pero no existe una política formal aprobada por la Alta Dirección.

Interpretación: requisito incumplido, Política de IA. Capítulo aplicable, Capítulo 5, Liderazgo. Conclusión: es una no conformidad frente a un requisito normativo obligatorio.

Este escenario suele evaluar dos confusiones típicas: creer que una política es deseable pero no obligatoria, y ubicarla en contexto, del Capítulo 4, en lugar de liderazgo, del Capítulo 5. La política pertenece al liderazgo porque expresa dirección y compromiso de la Alta Dirección y sirve de marco para objetivos.

Autoevaluación: ¿Este escenario corresponde al Capítulo 4 o al Capítulo 5?

Escenario 2 – Control no Justificado en la SoA

Situación: la organización excluye un control del Anexo A, pero no documenta la justificación.

Interpretación: documento afectado, Declaración de Aplicabilidad (SoA). Relación con Capítulo 6, tratamiento del riesgo. Conclusión: incumplimiento del requisito de trazabilidad y justificación. La exclusión sin sustento formal no cumple el requisito.

En Foundation, el foco no es si el control era bueno o malo, sino entender que el sistema exige decisiones justificadas. La SoA no puede ser una lista arbitraria: debe reflejar por qué se incluyen o excluyen controles en función del análisis y tratamiento del riesgo.

Autoevaluación: ¿La SoA puede omitir controles sin explicación formal?

Escenario 3 – No Evaluación de Riesgos tras Cambio

Situación: la organización modifica significativamente su modelo de IA, pero no actualiza la evaluación de riesgos.

Interpretación: requisito incumplido, evaluación de riesgos ante cambios. Capítulo aplicable: Capítulos 6 y 8, planificación y control operacional. Conclusión: falta de planificación y de control ante cambios significativos; los cambios activan una reevaluación obligatoria.

Este escenario mide comprensión de recurrencia: la evaluación de riesgos no es un evento único. Cuando cambian condiciones relevantes, como uso, datos, alcance o contexto, el SGIA debe responder con actualización y evidencia. Si no se actualiza, el sistema pierde su lógica de control.

Autoevaluación: ¿La evaluación de riesgos es un evento único o recurrente?

Escenario 4 – Auditoría Interna No Realizada

Situación: el SGIA está implementado, pero nunca se ha realizado auditoría interna.

Interpretación: capítulo aplicable, Capítulo 9, Evaluación del desempeño. Conclusión: incumplimiento de un requisito obligatorio; impacta la verificación de conformidad y eficacia del SGIA.

La auditoría interna no es opcional: es el mecanismo que permite comprobar si el sistema funciona como fue diseñado y si cumple los requisitos. En preguntas tipo examen, suele presentarse como ya operamos el SGIA para inducir la idea falsa de que la auditoría es un extra.

Autoevaluación: ¿La auditoría interna pertenece a operación o a evaluación del desempeño?

Escenario 5 – Corrección sin Acción Correctiva

Situación: se detecta una no conformidad y se corrige el error, pero no se analiza la causa raíz.

Interpretación: capítulo aplicable, Capítulo 10, Mejora. Conclusión: se realizó corrección, pero no acción correctiva completa. Es un cumplimiento parcial: el requisito exige análisis de causa y verificación de eficacia.

Este escenario suele evaluar un matiz clave: corregir elimina el síntoma; la acción correctiva elimina la causa para evitar recurrencia. Sin análisis causal, la organización no puede demostrar aprendizaje ni control de repetición.

Autoevaluación: ¿Corrección y acción correctiva son equivalentes?

Escenario 6 – Falta de Competencia Documentada

Situación: el equipo de IA afirma tener experiencia, pero no existe evidencia documentada de competencia.

Interpretación: capítulo aplicable, Capítulo 7, Soporte. Requisito incumplido: competencia y evidencia documentada. Conclusión: puede generar no conformidad en auditoría; la competencia debe demostrarse objetivamente.

Este tipo de pregunta distingue afirmaciones de evidencia. En sistemas ISO, la conformidad se demuestra mediante información documentada: registros de formación, perfiles, evaluaciones y asignaciones. La experiencia sin trazabilidad suele considerarse insuficiente.

💡 **TIP DE EXAMEN:** En preguntas de escenario, busca primero la evidencia faltante. En Foundation, la ausencia de evidencia documentada suele conducir al capítulo correcto con mayor rapidez que el detalle técnico del caso.

Autoevaluación: ¿La experiencia sin registro documental cumple el requisito?

Cierre del Módulo 5 – Preparación para el Examen

El Dominio E no evalúa profundidad técnica avanzada, sino capacidad de asociación conceptual: identificar el capítulo correcto, diferenciar entre requisito y control, y reconocer no conformidades en escenarios simples.

La estrategia clave consiste en identificar el concepto central del escenario, ubicarlo en el capítulo correspondiente y determinar si es requisito obligatorio o control de referencia.

Si dominas esta triada, podrás responder de forma consistente aun cuando la pregunta incluya distractores.

Autoevaluación final del Dominio E: ¿Podrías leer un escenario breve y ubicar el capítulo aplicable en menos de 20 segundos?

MÓDULO 6 – Cierre General, Estrategia de Examen y Recursos de Apoyo

Síntesis Integral de la Certificación I42001F™

A lo largo de esta guía se desarrollaron los cinco dominios evaluables del examen Foundation: Dominio A (25 %), terminología y propósito del SGIA; Dominio B (40 %), estructura de los capítulos 4–10; Dominio C (20 %), SoA y Anexos A/B/C/D; Dominio D (10 %), roles, partes interesadas y aplicabilidad; y Dominio E (5 %), interpretación básica en escenarios.

La certificación Foundation valida comprensión estructural, no implementación avanzada ni auditoría formal. La clave es entender el sistema como un todo integrado y dinámico: cómo se conectan contexto, liderazgo, planificación, operación, evaluación y mejora.

Autoevaluación: ¿Puedes explicar cómo se distribuye el peso del examen entre los cinco dominios?

Estrategia Final para Presentar el Examen

El examen es de opción múltiple, por lo que la estrategia debe centrarse en identificar el concepto central de la pregunta, ubicar el capítulo correspondiente, diferenciar entre requisito obligatorio y control de referencia, y descartar distractores conceptuales.

Errores frecuentes: confundir el Anexo A con requisito obligatorio absoluto, confundir corrección con acción correctiva y no distinguir riesgo de impacto.

Una recomendación práctica: cuando dudes entre dos opciones, pregúntate cuál de ellas respeta la jerarquía normativa, es decir, capítulos obligatorios versus anexos orientativos, y cuál describe un requisito verificable.

Autoevaluación: ¿Te sientes capaz de identificar rápidamente si una pregunta se refiere al Capítulo 6, 8 o 9?

Mapa Mental del SGIA para Repaso Final

Para repaso rápido, recuerda el ciclo PDCA aplicado al SGIA:

PLAN → Contexto (4) → Liderazgo (5) → Planificación (6)

DO → Soporte (7) → Operación (8)

CHECK → Evaluación del desempeño (9)

ACT → Mejora (10)

Si puedes reconstruir este esquema mentalmente, dominas el núcleo del Dominio B. Además, este mapa actúa como brújula para el examen: ante cualquier concepto, primero ubicas su fase PDCA y luego su capítulo.

Autoevaluación: ¿Puedes reconstruir el ciclo PDCA del SGIA sin consultar material?

Recursos Recomendados para Profundización

Para consolidar el aprendizaje: ISO/IEC 42001:2023, norma oficial; guías complementarias ISO/IEC sobre IA y gobernanza; ISO 19011, sobre auditoría de sistemas de gestión; publicaciones sobre gestión de riesgos en IA; y documentación oficial del esquema de certificación.

Este material es un recurso de apoyo voluntario y no sustituye la norma oficial. Dicho esto, revisar el texto normativo ayuda a reforzar definiciones, estructura y lenguaje, especialmente en los dominios A, B y C.

Autoevaluación: ¿Has revisado directamente el texto de la norma para reforzar conceptos clave?

Cierre General – Competencia Esperada del Profesional I42001F™

Al finalizar esta preparación deberías ser capaz de explicar qué es un SGIA y su propósito, describir la estructura de ISO/IEC 42001, comprender la función de la SoA y los anexos, identificar responsabilidades organizacionales e interpretar escenarios simples conforme a la norma.

La certificación Foundation acredita comprensión estructural y capacidad de interpretación básica del estándar. El siguiente nivel de madurez profesional implica implementación o auditoría del SGIA, donde se requieren habilidades adicionales de diseño, evidencia y verificación sistemática.

Autoevaluación final: ¿Podrías explicar ISO/IEC 42001 a un colega en menos de cinco minutos con claridad y precisión?

¿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

#I42001F #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com