

CERTIFICACIÓN · INTELIGENCIA ARTIFICIAL

ISO/IEC 42001: sistema de gestión para la IA

Si entrega funciones de IA a clientes de la UE, le van a preguntar por datos, riesgos y control. ISO/IEC 42001 es la primera norma internacional con la que puede dar una respuesta ordenada.

VERSIÓN VIGENTE	OBJETO	VIGENCIA	RELACIÓN
ISO/IEC 42001:2023	sistema de gestión de inteligencia artificial (AIMS)	3 años, auditorías de seguimiento anuales	Reglamento de IA (UE) 2024/1689

En pocas palabras

ISO/IEC 42001 establece los requisitos de un sistema de gestión de inteligencia artificial, AIMS por su sigla en inglés. La norma salió a fines de 2023. Está dirigida a organizaciones que desarrollan, ofrecen o utilizan sistemas de IA y sigue la misma estructura básica que ISO/IEC 27001 e ISO 9001. Quien conoce alguna de esas normas se orienta rápido.

En el centro están las preguntas que los clientes de la UE hacen a los proveedores de IA: ¿qué sistemas de IA opera, para qué y con qué datos? ¿Qué riesgos surgen para las personas afectadas y quién decide sobre ellos? ¿Cómo supervisa los modelos en operación y qué pasa cuando se equivocan? La norma exige una evaluación de impacto de los sistemas de IA, un tratamiento de riesgos y controles que se enumeran en un anexo, de forma parecida a ISO/IEC 27001.

La norma es neutral en cuanto a la tecnología. Se aplica tanto a un modelo propio para pronosticar rendimientos de cosecha como a un chatbot de atención al cliente construido sobre un modelo de lenguaje contratado. El segundo caso es frecuente en Sudamérica: muchos proveedores no desarrollan modelos base propios, sino que arman productos sobre modelos de grandes proveedores. ISO/IEC 42001 exige entonces que usted gestione también a esos proveedores, conozca sus límites y documente cómo maneja los errores del modelo.

Por qué la piden los clientes de la UE

El [Reglamento de Inteligencia Artificial](#) de la UE se aplica también a proveedores de fuera de la UE cuando introducen sistemas de IA en el mercado de la UE o cuando la información de salida de un sistema se usa en la UE (art. 2). Una empresa de software de Buenos Aires que construye para una

aseguradora española un modelo de evaluación de siniestros queda alcanzada con facilidad. Las obligaciones entran en vigor de forma escalonada; las prohibiciones rigen desde febrero de 2025 y las reglas para modelos de IA de uso general, desde agosto de 2025. Los demás plazos y su estado actual están en nuestra página sobre el Reglamento de IA.

Según el Reglamento, los proveedores de IA de alto riesgo necesitan, entre otras cosas, un sistema de gestión de la calidad, gestión de riesgos, documentación técnica y supervisión humana. ISO/IEC 42001 cubre muchos de estos temas a nivel de organización. Pero un certificado no significa que un sistema de IA cumpla el Reglamento de IA. Qué normas otorgan presunción de conformidad se desprende de las normas armonizadas que se publican en el Diario Oficial de la UE. Aun así, para sus clientes de la UE el certificado es una señal fuerte de que usted gestiona la IA de manera ordenada.

Además siguen vigentes las reglas conocidas. Si se tratan datos personales, por ejemplo para el entrenamiento, rige el [RGPD \(Reglamento General de Protección de Datos\)](#). Si el sistema de IA funciona en un banco o una aseguradora, se suma [DORA](#) a través de su cliente.

Quién la necesita en Sudamérica

- Startups de IA y empresas de software en São Paulo, Santiago, Bogotá, Medellín, Buenos Aires o Montevideo que venden productos de IA a clientes de la UE
- Proveedores de ciencia de datos y analítica que entrenan u operan modelos para mandantes europeos
- BPO y contact centers que usan chatbots o decisiones automatizadas para clientes de la UE
- Fintechs con scoring, detección de fraude o verificación de identidad
- Empresas agritech con análisis de imágenes o satelitales, por ejemplo para la trazabilidad exigida por el [EUDR](#)
- Empresas de recursos humanos que usan IA para seleccionar o evaluar postulantes

El camino hasta la certificación

1. Armar un inventario de todos los sistemas de IA: finalidad, fuentes de datos, modelos, terceros involucrados y su rol (desarrollador, proveedor, usuario).
2. Definir el alcance del AIMS y aprobar las políticas de IA.
3. Evaluar los riesgos y los impactos para las personas afectadas y la sociedad, seleccionar y fundamentar los controles.
4. Implementar procesos de calidad de datos, desarrollo, pruebas, aprobación, supervisión en operación e incidentes.

5. Operar el sistema durante algunos meses, realizar la auditoría interna y la revisión por la dirección.
6. Auditorías de etapa 1 y etapa 2 a cargo de un organismo certificador acreditado.
7. Certificado por tres años, con auditorías de seguimiento anuales.

Lo habitual son entre 6 y 12 meses. Si ya opera un SGSI según ISO/IEC 27001, puede aprovechar el control de documentos, las auditorías y la gestión de proveedores, y a menudo avanza más rápido. Los costos dependen de la cantidad y el tipo de sistemas de IA y varían mucho. Empiece por los sistemas que afectan a clientes de la UE y amplíe el alcance más adelante, cuando el sistema ya funcione en el día a día.

Acreditación: qué organismo cuenta

El organismo certificador debería estar acreditado expresamente para ISO/IEC 42001 por un organismo de acreditación firmante del acuerdo internacional de reconocimiento. Hasta fines de 2025 era el IAF MLA; desde el 1 de enero de 2026 es el MRA de la Global Accreditation Cooperation Incorporated (Global ACI). Con una norma tan reciente conviene revisar con especial atención el certificado de acreditación: no todo organismo que certifica ISO/IEC 27001 está acreditado también para ISO/IEC 42001.

PAÍS	ORGANISMO DE ACREDITACIÓN
Argentina	OAA, Organismo Argentino de Acreditación
Bolivia	DTA-IBMETRO, Dirección Técnica de Acreditación del Instituto Boliviano de Metrología
Brasil	Cgcre (Coordenação-Geral de Acreditação) del INMETRO
Chile	INN, Instituto Nacional de Normalización
Colombia	ONAC, Organismo Nacional de Acreditación de Colombia
Ecuador	SAE, Servicio de Acreditación Ecuatoriano
Paraguay	ONA, Organismo Nacional de Acreditación (del CONACYT)
Perú	INACAL, Dirección de Acreditación
Uruguay	OUA, Organismo Uruguayo de Acreditación

Los nueve organismos figuran en la Global ACI como firmantes (al 11/10/2026). Si alguno de ellos ya acreditó organismos certificadores para ISO/IEC 42001 es algo que hay que verificar caso por caso. Un organismo certificador con acreditación de otro país firmante se reconoce igual.

Errores frecuentes

- El inventario de IA está incompleto. Faltan los modelos de lenguaje de terceros integrados o la IA incluida en herramientas compradas.
- El certificado se presenta como prueba de conformidad con el Reglamento de IA. Los clientes de la UE con área legal propia lo notan.
- La evaluación de impacto considera solo los riesgos técnicos y no los efectos sobre las personas acerca de las cuales decide el sistema.
- Falta la supervisión en operación: los modelos se aprueban y después nadie los vuelve a revisar.
- La gestión de la IA va por separado de la protección de datos y la seguridad de la información, aunque se trata de los mismos datos y sistemas.
- No se revisan los contratos con los proveedores de modelos. Ahí dice si los datos de clientes pueden reutilizarse para entrenamiento, y eso es justamente lo que pregunta su cliente de la UE.
- La responsabilidad no está definida. Si nadie puede detener un sistema de IA que da resultados erróneos, cualquier auditor lo ve como una brecha.

Cómo ayuda Sightadel

[Sightadel](#) reúne en un solo lugar el inventario de IA, los riesgos, las evaluaciones de impacto, los controles y las evidencias, y los vincula con ISO/IEC 27001 y la protección de datos si ya existen. Con un [paquete de consultoría](#), consultores con experiencia lo acompañan hasta la certificación.

FAQ

¿Con ISO/IEC 42001 cumplimos el Reglamento de IA?

No de forma automática. La norma cubre muchos requisitos organizativos. Las obligaciones para cada sistema de IA, como la documentación técnica o el etiquetado, siguen siendo tareas aparte.

¿Nos aplica el Reglamento de IA si estamos fuera de la UE?

Sí, si ofrece sistemas de IA en la UE o si la información de salida de su sistema se usa en la UE. Los detalles están en nuestra página sobre el Reglamento de IA.

¿Necesitamos primero ISO/IEC 27001?

No, las normas se pueden certificar de forma independiente. Pero un SGSI existente facilita mucho ISO/IEC 42001, porque la estructura y muchos procesos son iguales.

¿Qué herramienta ayuda a armar el sistema de gestión de IA?

Sightadel trae ISO/IEC 42001 y el Reglamento de IA de la UE como marcos, con plantillas para el inventario de IA, la evaluación de impacto y los controles. Si ya trabaja con ISO/IEC 27001 en la plataforma, aprovecha lo hecho. El certificado lo emite después un organismo acreditado.

Fuentes · Actualizado: 11 de octubre de 2026

ISO: ISO/IEC 42001:2023: <https://www.iso.org/standard/42001>

Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial): <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Reglamento (UE) 2016/679 (RGPD): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Global ACI: organismos de acreditación reconocidos: <https://global-aci.org/en/recognised-abs/>

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por ISO 42001: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>