

ISO 42001 Guía de Implementación

Estándar internacional para sistemas de gestión de IA. Guía práctica para organizaciones de cualquier tamaño.

proyectosdelA.com

¿Qué es la ISO 42001?

La ISO/IEC 42001:2023 es el primer estándar internacional para Sistemas de Gestión de Inteligencia Artificial (SGAIA). Publicada en diciembre de 2023 por la Organización Internacional de Normalización (ISO), establece un marco para que las organizaciones desarrollen, implementen, mantengan y mejoren continuamente su gestión responsable de la IA.

¿Es obligatoria?

No. La ISO 42001 es voluntaria. Sin embargo, implementarla facilita el cumplimiento del AI Act, demuestra madurez en gobernanza de IA, puede ser requerida por clientes corporativos o en licitaciones, y es certificable — lo que permite diferenciarse en el mercado.

Relación con el AI Act

ISO 42001 y AI Act son complementarios. El AI Act establece los mínimos legales obligatorios. La ISO 42001 proporciona el sistema de gestión para cumplirlos y superarlos. Una empresa certificada en ISO 42001 tiene implementado el 60-70% de lo que exige el AI Act para sistemas de alto riesgo.

La estructura de la ISO 42001

Sigue la estructura de alto nivel (HLS) común a todas las normas ISO de gestión (9001, 27001, 14001). Esto facilita la integración con sistemas de gestión ya existentes.

CLÁUSULA	TÍTULO	CONTENIDO PRINCIPAL
4	Contexto de la organización	Entender el contexto interno y externo. Identificar partes interesadas. Definir el alcance del sistema de gestión. Establecer políticas de IA.
5	Liderazgo	Compromiso de la alta dirección. Política de IA aprobada por dirección. Roles, responsabilidades y autoridades definidas.
6	Planificación	Identificar riesgos y oportunidades de la IA. Establecer objetivos de gobernanza. Planificar los cambios necesarios.
7	Apoyo	Recursos asignados. Competencias del personal definidas. Comunicación interna y externa. Documentación controlada.
8	Operación	Planificación y control operativo. Evaluación de impacto de sistemas de IA. Controles para el uso responsable de IA. Gestión de proveedores.
9	Evaluación del desempeño	Seguimiento y medición. Auditoría interna. Revisión por la dirección.
10	Mejora	No conformidades y acciones correctivas. Mejora continua del sistema.

Los controles específicos de IA (Anexo A)

La ISO 42001 incluye 38 controles específicos para la gestión de sistemas de IA, organizados en 9 categorías. Son el corazón práctico del estándar.

REF.	CATEGORÍA DE CONTROL	DESCRIPCIÓN
A.2	Políticas para IA	Política de IA, objetivos, roles y responsabilidades formalizados.
A.3	Recursos internos de IA	Gestión del conocimiento, competencias y recursos para operar la IA.
A.4	Ciclo de vida de la IA	Gestión desde el diseño hasta el retiro de los sistemas de IA.
A.5	Evaluación de impacto en la sociedad	Análisis del impacto de la IA en personas, grupos y sociedad.

A.6	Gestión de datos de IA	Calidad, sesgo, privacidad y gobierno de los datos usados.
A.7	Diseño y desarrollo de sistemas de IA	Controles para el desarrollo responsable de sistemas.
A.8	Información para usuarios de IA	Transparencia hacia usuarios y partes afectadas.
A.9	Uso de sistemas de IA	Controles para el despliegue y operación responsable.
A.10	Terceros e IA	Gestión de proveedores y cadena de suministro de IA.

Hoja de ruta de implementación

Implementar la ISO 42001 es un proyecto de 6-18 meses dependiendo del tamaño de la organización y su madurez previa.

FASE	TÍTULO	ACTIVIDADES PRINCIPALES
FASE 1 (Mes 1-2)	Diagnóstico	Evaluar el nivel actual de madurez. Identificar brechas respecto a la norma. Definir alcance y equipo del proyecto.
FASE 2 (Mes 2-4)	Políticas y roles	Aprobar política de IA. Definir roles y responsabilidades. Inventario de sistemas de IA.
FASE 3 (Mes 4-8)	Implementación	Implementar controles del Anexo A. Evaluar impactos. Formar al equipo. Documentar procesos.
FASE 4 (Mes 8-12)	Operación y mejora	Operar el sistema. Auditoría interna. Revisión por dirección. Acciones correctivas.
FASE 5 (Mes 12-18)	Certificación	Auditoría de certificación por organismo acreditado (ENAC en España). Obtención del certificado.

ISO 42001 vs AI Act: cuándo necesita ambos

Si su empresa tiene sistemas de alto riesgo, necesita cumplir el AI Act (obligatorio). Si además quiere demostrar madurez, diferenciarse en el mercado y tener un sistema de mejora continua, la ISO 42001 es el siguiente paso natural. El trabajo de cumplimiento del AI Act cubre el 60-70% de la ISO 42001 — no es empezar de cero.