CUADERNO DE PRÁCTICA

# ISO/IEC 27090:2026 · Ciberseguridad e IA

Ficha de revisión de un asistente jurídico

Fuentes revisadas: 2026-10-21 · Edición de lectura y trabajo.

## Tu recorrido de trabajo

01. Finalidad y resultado permitido

02. Datos autorizados y datos excluidos

03. Proveedor, modelo y versión

04. Fuentes documentales y fecha de revisión

05. Herramientas y permisos concedidos

06. Persona que revisa y puede detener la operación

07. Tres pruebas de error o manipulación y resultados

08. Qué sucede si la fuente o el modelo cambian

### Resultado esperado

La ficha identifica responsables, límites y evidencia de prueba; ninguna acción sensible se ejecuta solo porque la respuesta del modelo parezca convincente.

## Antes de darlo por terminado

01. Finalidad y responsables identificados.

02. Datos y herramientas delimitados.

03. Casos de prueba registrados y revisión humana.

## Registro de contraste

### Pregunta concreta y hechos disponibles

### Fuente original, fecha, ámbito y apartado

### Conclusión provisional y límite de la evidencia

### Revisión humana, responsable y condición para detener el uso

## Fuentes para el ejercicio

### ISO, ficha oficial ISO/IEC 27090:2026

https://www.iso.org/standard/27090

### IEC, ISO/IEC 27090:2026

https://webstore.iec.ch/en/publication/117332

### ISO/IEC 27001:2022

https://www.iso.org/standard/27001

### ISO/IEC 42001:2023

https://www.iso.org/standard/42001

### ISO/IEC 23894:2023

https://www.iso.org/standard/77304.html

### NIST AI 100-2e2025, taxonomía de aprendizaje automático adversarial

https://www.nist.gov/publications/adversarial-machine-learning-taxonomy-and-terminology-attacks-and-mitigations-0

### OWASP, riesgos de aplicaciones LLM y GenAI

https://genai.owasp.org/llm-top-10/

### OWASP, autonomía excesiva

https://genai.owasp.org/llmrisk/llm062025-excessive-agency/?lang=us

### NIST, AI Agent Standards Initiative

https://www.nist.gov/news-events/news/2026/02/announcing-ai-agent-standards-initiative-interoperable-and-secure

### NIST, síntesis de respuestas sobre seguridad de agentes

https://www.nist.gov/publications/summary-analysis-responses-request-information-regarding-security-considerations-ai

### NIST IR 8607, Cyber AI Profile Workshop

https://www.nist.gov/publications/workshop-summary-report-cyber-ai-profile-hybrid-workshop

Abrir la guía completa y sus actualizaciones