

GUÍA DE ESTUDIO

ISO/IEC 27090:2026 · Ciberseguridad e IA

ISO/IEC 27090:2026 orienta el tratamiento de amenazas de seguridad propias de sistemas de IA a lo largo de su ciclo de vida. Se dirige a organizaciones que desarrollan o utilizan estos sistemas. Esta página explica su alcance público y propone ejercicios educativos originales; no reproduce el texto de la norma ni acredita cumplimiento.

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

Qué cambió con esta publicación

La nueva referencia permite tratar de forma específica la seguridad de los sistemas de IA, en lugar de asumir que toda amenaza se resuelve únicamente con los controles habituales de una aplicación. El alcance público incluye comprender las consecuencias, detectar y mitigar amenazas durante el ciclo de vida. No convierte por sí sola una aplicación en segura ni reemplaza una evaluación concreta. En una organización jurídica deben revisarse además las normas aplicables, los datos tratados, las obligaciones contractuales y las reglas de la entidad. Un resumen educativo no acredita conformidad.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

El riesgo cambia cuando el asistente puede actuar

Una respuesta errónea puede convertirse en un daño operativo si la herramienta también puede enviar correos, modificar archivos o ejecutar otras acciones. Por eso conviene establecer permisos desde el sistema que recibe la acción y no confiar exclusivamente en que el modelo recuerde una prohibición. La práctica propuesta es separar tres etapas: recuperar información autorizada, preparar un borrador y obtener revisión antes de ejecutar una acción sensible. El criterio debe adaptarse al impacto; las decisiones jurídicas siguen bajo responsabilidad de la persona competente.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

Datos, corpus y fuentes también forman parte del sistema

La calidad de un asistente no depende solo de su modelo. Un repositorio alterado, una fuente desactualizada o un documento externo con instrucciones maliciosas pueden contaminar la respuesta. Una fuente recuperada mediante RAG requiere revisión de procedencia y pertinencia. Para una biblioteca jurídica, registrar edición, fecha y enlace de cada documento; limitar quién puede incorporar materiales y conservar un historial de cambios. Estas son recomendaciones prácticas, no cláusulas reproducidas de la norma.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

Un piloto prudente para una oficina jurídica

Elegir una tarea de impacto acotado: comparar el índice de dos documentos públicos o elaborar preguntas de lectura. Definir qué datos se permiten y qué acciones se excluyen. Crear un pequeño conjunto de pruebas con resultado esperado y revisar falsos positivos y omisiones. Antes de ampliar el piloto, exigir evidencia de que el sistema mantiene el alcance previsto. Si el proveedor cambia de versión, repetir las pruebas relevantes. Un aumento de productividad declarado debe sustentarse con una medición propia, no con cifras promocionales.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

Lectura actual: agentes y ciberseguridad en 2026

NIST anunció su iniciativa de estándares para agentes el 17 de febrero de 2026. En mayo publicó una síntesis de respuestas sobre seguridad de agentes. Es evidencia de una agenda de investigación y normalización, no una garantía de que todos los controles ya estén maduros. En agosto de 2026 NIST publicó el informe del taller Cyber AI Profile. Resume discusiones para orientar el desarrollo del perfil e incluye oportunidades y retos de la defensa apoyada en IA. Un informe de taller no debe presentarse como una norma final obligatoria.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

Antes de afirmar cumplimiento

Definir el alcance de la afirmación, obtener el texto autorizado y revisar la evidencia aplicable con personal competente. No ofrecer un sello de conformidad por completar una infografía o una lista de comprobación. En Colombia, la existencia de un estándar internacional no permite afirmar por sí sola que todas las organizaciones estén obligadas a aplicarlo. La exigibilidad en un caso requiere identificar una norma, contrato u otra fuente concreta. Esta página no ofrece un dictamen sobre ese supuesto.

Consultar documento de soporte: www.iso.org

Consultar documento de soporte: webstore.iec.ch

Llévalo a la práctica

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.

Método y alcance

Síntesis educativa del catálogo oficial público y fuentes técnicas complementarias; no reproduce el texto completo de la norma de pago ni acredita conformidad.

Fuentes originales

01. ISO, ficha oficial ISO/IEC 27090:2026

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

Fuente técnica primaria

02. IEC, ISO/IEC 27090:2026

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

Fuente técnica primaria

03. ISO/IEC 27001:2022

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

Fuente técnica primaria

04. ISO/IEC 42001:2023

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

Fuente técnica primaria

05. ISO/IEC 23894:2023

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

Fuente técnica primaria

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

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

Fuente técnica primaria

07. OWASP, riesgos de aplicaciones LLM y GenAI

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

Fuente técnica primaria

08. OWASP, autonomía excesiva

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

Fuente técnica primaria

09. NIST, AI Agent Standards Initiative

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

Fuente técnica primaria

10. NIST, síntesis de respuestas sobre seguridad de agentes

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

Fuente técnica primaria

11. NIST IR 8607, Cyber AI Profile Workshop

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

Fuente técnica primaria

Continúa en la web

<https://alejoqqa.com/temas/iso-iec-27090-2026.html>

Consulta la versión web para actualizaciones posteriores a la fecha de revisión.