

Inteligencia Artificial: nuestros servicios



Inteligencia Artificial

Normativa aplicable

El **Reglamento (UE) 2024/1689 de Inteligencia Artificial (RIA)**, es la primera ley integral sobre IA a nivel mundial que establece un enfoque basado en el riesgo, con obligaciones tanto para quien desarrolla los sistemas (proveedor) como para quien los utiliza (responsable del despliegue), que se resumen a continuación:



La IA no solo implica riesgos y oportunidades a nivel tecnológico y operativo, se trata de un nuevo modelo de gestión, sujeto a requerimientos regulatorios y de gobierno corporativo.



PRÁCTICAS PROHIBIDAS	ALFABETIZACIÓN EN IA	MODELOS DE USO GENERAL (GPAI)	TRANSPARENCIA (ART. 50)	SISTEMAS DE ALTO RIESGO
Eliminar los usos de riesgo inaceptable: puntuación social, manipulación o reconocimiento de emociones en el trabajo. Aplica a: Todos los operadores	Promover un nivel suficiente de conocimientos en IA del personal que utiliza o supervisa los sistemas. Aplica a: Proveedores y usuarios	Documentación técnica, política de derechos de autor y resumen de datos de entrenamiento; requisitos reforzados si hay riesgo sistémico. Aplica a: Proveedores de modelos	Informar de que se interactúa con una IA y marcar o etiquetar el contenido generado (p. ej., <i>deepfakes</i>). Aplica a: Proveedores y usuarios	Gestión de riesgos, gobierno del dato, documentación, supervisión humana y ciberseguridad; FRiA en ciertos casos. Aplica a: Proveedores y usuarios
2 feb 2025 - En vigor	2 feb 2025 - En vigor	2 ago 2025 - En vigor	2 ago 2026 - En vigor	2 dic 2027* - Próximamente

Usuarios = responsables del despliegue. Marcado de contenido generado por IA ya comercializada: 2 dic 2026.
* Alto riesgo aplazado por el Omnibus Digital sobre IA (inicialmente 2 ago 2026); en productos regulados (Anexo I): 2 ago 2028.

MARCO NORMATIVO Y SUPERVISIÓN EN ESPAÑA

A continuación, se recogen algunos de los **organismos y normativa de interés a nivel nacional**:

- ▶ **AESIA** (Agencia Española de Supervisión de la IA) autoridad de vigilancia del mercado, junto con la AEPD y los supervisores sectoriales.
- ▶ **Proyecto de Ley Orgánica para el buen uso y la gobernanza de la IA** (Consejo de Ministros, mayo 2026), en tramitación parlamentaria: régimen sancionador nacional, *sandboxes* y obligaciones adicionales (p.ej., etiquetado de *deepfakes*).
- ▶ **Interacción con otras normas**: RGPD, DORA, NIS2 y normativa sectorial (financiera, laboral, consumo), que exigen un enfoque de cumplimiento integrado.

ISO/IEC 42001: LA BUENA PRÁCTICA DE MERCADO

Publicada en diciembre de 2023, es la **primera norma internacional certificable** para Sistemas de Gestión de la IA (SGIA).

- ▶ Adopción acelerada: **MÁS DE 350 ORGANIZACIONES CERTIFICADAS EN EL MUNDO** (abril 2026), entre ellas AWS, Microsoft, KPMG o BCG; en España ya se certifica a través de entidades como AENOR.
- ▶ Se ha convertido en la referencia para demostrar un uso responsable de la IA ante clientes, reguladores y en la evaluación de proveedores.
- ▶ No otorga presunción de conformidad con el RIA, pero cubre buena parte de sus exigencias de gobierno, gestión de riesgos y supervisión humana.
- ▶ Como paso previo o marco progresivo hacia la certificación ISO/IEC 42001, en España existe la certificación de "Compromiso con la IA Responsable" de AENOR EP 40201:2025. Esta Especificación Privada recoge buenas prácticas que no llegan a ser el estándar ISO internacional, pero es una buena referencia de inicio.

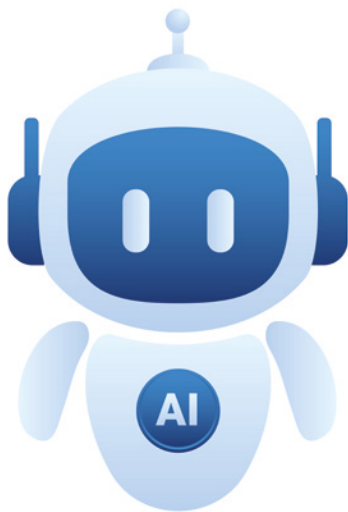
Inteligencia Artificial

Regimen sancionador

El RIA acompaña sus obligaciones con un **régimen sancionador especialmente severo**, con multas que superan a las del RGPD y que se gradúan según la gravedad del incumplimiento. Los Estados miembros fijan las normas nacionales y velan por su aplicación: **en España, la AESIA y las autoridades sectoriales, conforme al futuro régimen de la Ley Orgánica de IA.**



SANCIONES MÁXIMAS DEL RIA: UN RÉGIMEN ESCALONADO SEGÚN LA GRAVEDAD



35 M€ O 7 % de la facturación mundial anual

PRÁCTICAS DE IA PROHIBIDAS (ART. 5)

Manipulación subliminal, explotación de vulnerabilidades, puntuación social, reconocimiento de emociones en el trabajo o la educación, categorización biométrica sensible.

Ej.: herramienta de selección que infiere las emociones de los candidatos durante la entrevista.

7,5 M€ O 1 % de la facturación mundial anual

INFORMACIÓN INCORRECTA A LAS AUTORIDADES

Facilitar información inexacta, incompleta o engañosa a los organismos notificados o a las autoridades nacionales competentes.

Ej.: documentación técnica o inventario de sistemas inexacto aportado en una inspección.

15 M€ O 3 % de la facturación mundial anual

INCUMPLIMIENTO DE OTRAS OBLIGACIONES

Requisitos de los sistemas de alto riesgo (gestión de riesgos, datos, documentación, supervisión humana), obligaciones de proveedores, importadores, distribuidores y responsables del despliegue, y transparencia (art. 50).

Ej.: chatbot que no informa al usuario de que interactúa con una IA, o modelo de scoring crediticio sin supervisión humana.

Se aplica la cifra fija o el porcentaje sobre la facturación mundial del ejercicio anterior, la que sea mayor (para pymes y startups, la menor). Las multas a proveedores de modelos de IA de uso general (hasta 15 M€ o 3 %) las impone directamente la Comisión Europea (art. 101). Régimen aplicable desde el 2 de agosto de 2025.



ASPECTOS CLAVE DEL RÉGIMEN SANCIONADOR:

Por encima del RGPD

El techo del RIA (35 M€ / 7 %) casi duplica el del RGPD (20 M€ / 4 %), y ambas sanciones pueden concurrir si el sistema trata datos personales.

Criterios de graduación

Naturaleza, gravedad y duración de la infracción, personas afectadas, cooperación con la autoridad, medidas de mitigación, reincidencia y tamaño del infractor.

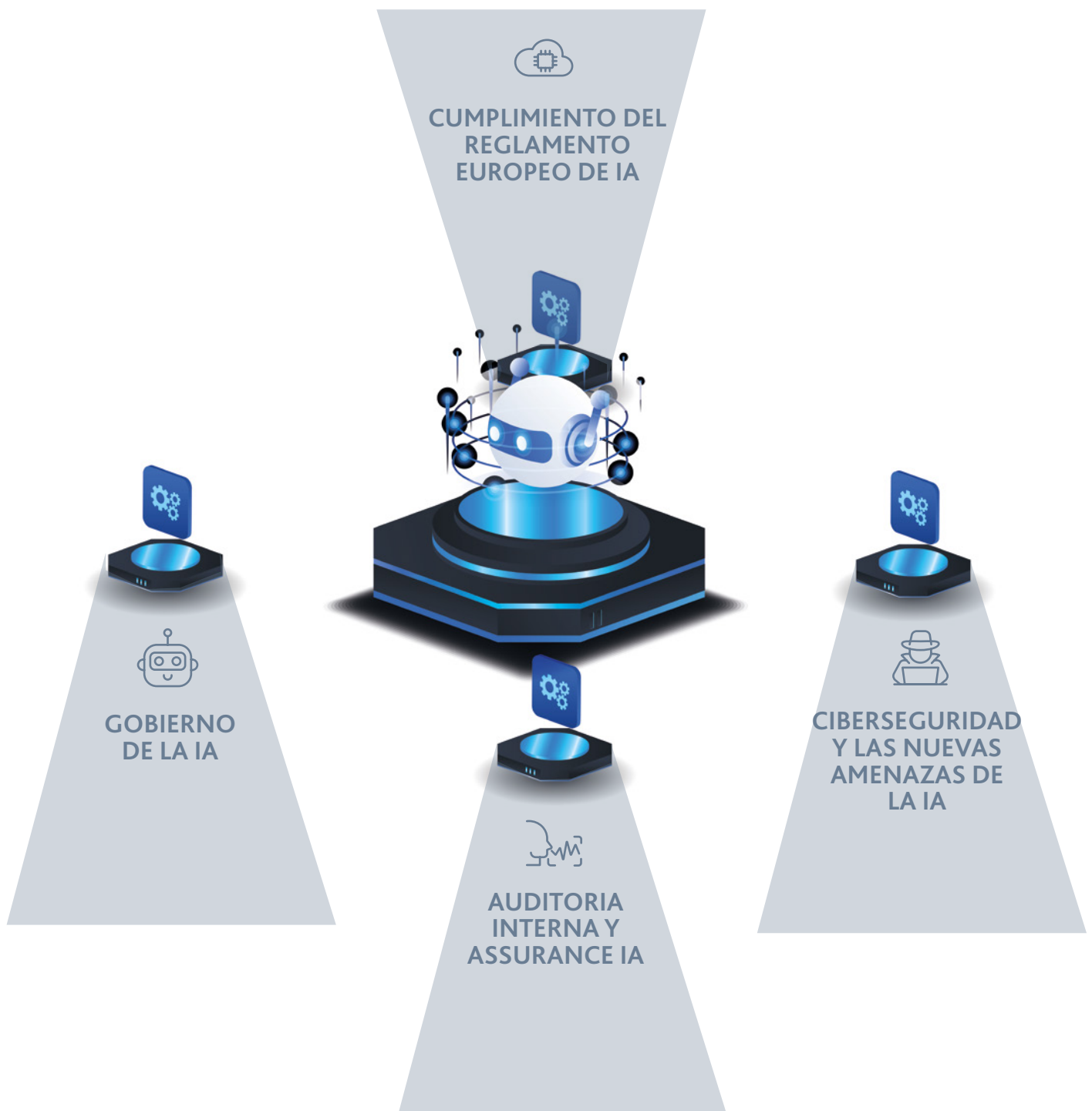
Más allá de la multa

Retirada o prohibición del uso del sistema, retirada de certificaciones y licencias, e incluso responsabilidad civil y penal, con el consiguiente daño reputacional, pérdida de confianza de clientes e inversores y exposición de los órganos de gobierno.

Inteligencia Artificial

Nuestros servicios

Acompañamos a las organizaciones en el diseño de un **marco de gobierno de la IA** integrado en su Sistema de Control Interno y en su adaptación al **Reglamento (UE) 2024/1689 de Inteligencia Artificial (RIA)**, desde el diagnóstico inicial hasta la auditoría y la certificación.



Inteligencia Artificial

Nuestros servicios



GOBIERNO DE LA IA

Análisis de riesgos de procesos con IA

Inventario de sistemas y modelos de IA, clasificación por criticidad y evaluación de impactos (negocio, operativo, ético y de privacidad). Evaluación de riesgos operativos, regulatorios, éticos y de privacidad.

Modelo de gobierno de la IA

Políticas y códigos de uso, roles y comité de IA, integración de controles en el SCI y cuadro de mando de KPI/KRI para su monitorización.

Sistema de Gestión de IA (ISO/IEC 42001)

Diagnóstico de madurez y análisis GAP.
Diseño e implantación del SGIA.
Auditoría interna y preparación para certificación.

CUMPLIMIENTO DEL REGLAMENTO EUROPEO DE LA IA



Análisis gap y plan de acción

Clasificación de los sistemas por nivel de riesgo y rol de la entidad (proveedor o responsable del despliegue), brechas y hoja de ruta priorizada.

Auditorías externas de cumplimiento

Verificación independiente de requisitos: gestión de riesgos, gobernanza de datos, documentación técnica, transparencia y supervisión humana.

Acompañamiento en la implantación

Oficina de proyecto, documentación y procedimientos, programas de alfabetización en IA y seguimiento de medidas hasta su cierre.
Formación en IA .

Inteligencia Artificial

Nuestros servicios

A medida que la IA se integra en procesos críticos de negocio, los órganos de gobierno requieren una evaluación independiente de los riesgos, controles y mecanismos de supervisión implantados. Proporcionamos servicios de Auditoría Interna y Assurance para reforzar la confianza en el uso de la IA.



AUDITORIA INTERNA Y ASSURANCE IA

Auditoría de sistemas y casos de uso de IA

Revisión independiente de los sistemas de IA utilizados en procesos críticos.

Evaluación de riesgos operativos, financieros, tecnológicos y regulatorios asociados a la IA.

Verificación de la existencia y efectividad de controles clave durante todo el ciclo de vida de la IA.

Validación de modelos y calidad de resultados

Evaluación de la fiabilidad, robustez y consistencia de los resultados generados por la IA.

Revisión de controles sobre calidad, trazabilidad e integridad de los datos utilizados.

Identificación de riesgos de sesgo, degradación del modelo y desviaciones respecto al uso previsto.

SOC 2 y confianza digital en soluciones de IA

Emisión de informes SOC 2 sobre servicios y plataformas que incorporan IA.

Validación de controles clave que permitan demostrar confianza, transparencia y cumplimiento frente a clientes y reguladores.

Revisión de riesgos asociados a proveedores y modelos de IA de terceros.

NUESTRO ENFOQUE:

1.

EVALUACIÓN DE RIESGOS
Y ALCANCE

2.

REVISIÓN DE CONTROLES
Y EVIDENCIAS

3.

INFORME
INDEPENDIENTE

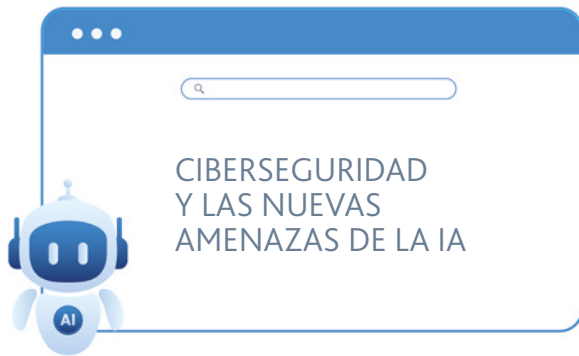
4.

SEGUIMIENTO Y MEJORA
CONTINUA

Inteligencia Artificial

Nuestros servicios

La IA amplía la superficie de ataque y acelera las amenazas. Ayudamos a adaptar el marco de defensa y respuesta, a controlar el uso no autorizado de la IA y a aprovecharla en las operaciones de seguridad.



GOBIERNO DE LA IA

Defensa y respuesta ante ataques de IA

Evaluación de la exposición a amenazas potenciadas por IA: *phishing* personalizado, *deepfakes* y *malware* polimórfico.

Pruebas adversariales y red teaming sobre modelos (*prompt injection*, envenenamiento de datos).

Actualización del marco de defensa, planes de respuesta y *playbooks*.

Riesgos del "shadow IA" y agentes sin control

Descubrimiento del uso de herramientas de IA no autorizadas.

Inventario de agentes de IA, sus permisos y accesos a datos y sistemas.

Políticas de uso aceptable, controles DLP y gestión de identidades no humanas.

IA aplicada a la defensa: SOC aumentado

Automatización del triaje y la correlación de alertas.

Reducción de los tiempos de detección y respuesta (MTTD/MTTR).

Threat hunting asistido y evaluación de herramientas de IA en el SOC.

NUESTRO ENFOQUE:

1.

DIAGNÓSTICO
DE EXPOSICIÓN

2.

DISEÑO DE CONTROLES
Y RESPUESTA

3.

IMPLANTACIÓN
Y PRUEBAS

4.

MONITORIZACIÓN
CONTINUA

PARA MÁS INFORMACIÓN:

GONZALO GARCÍA-LIÑÁN

Socio | Risk Advisory Services
gonzalo.garcia-linan@bdo.es

Esta publicación ha sido redactada en términos generales y debe ser contemplada únicamente como una referencia general. Esta publicación no puede utilizarse como base para amparar situaciones específicas y usted no debe actuar, o abstenerse de actuar, de conformidad con la información contenida en este documento sin obtener asesoramiento profesional específico. Póngase en contacto con BDO en cualquiera de nuestras oficinas para tratar estos asuntos en el marco de sus circunstancias particulares. BDO, sus socios y empleados, no aceptan ni asumen cualquier responsabilidad ante cualquier pérdida derivada de cualquier acción realizada o no por cualquier individuo al amparo de la información contenida en esta publicación o ante cualquier decisión basada en ella.

BDO Auditores, S.L.P. es una sociedad limitada española independiente y miembro de la red internacional de BDO, constituida por empresas independientes asociadas de todo el mundo, y creada por BDO International Limited, una compañía limitada por garantía del Reino Unido.

BDO es la marca comercial utilizada por toda la red BDO y para todas sus firmas miembro.

Copyright © 2026. Todos los derechos reservados. Publicado en España.

bdo.es
bdo.global