RenLayer

INFORME DE CUMPLIMIENTO · ESPAÑA 2026

Ley de IA en España

Qué exige la nueva normativa a las empresas y cómo evitar sanciones de hasta 35 M€ o el 7 % de la facturación.

Una guía para los equipos de dirección, cumplimiento y seguridad, con una hoja de ruta para cumplir antes de que el régimen sancionador entre en plena aplicación, el 2 de agosto de 2026.

35 M€
Sanción máxima, hasta el 7 % de la facturación anual mundial

2 ago
Plena aplicación del régimen sancionador en 2026

10
Prácticas de IA prohibidas (riesgo inaceptable)

AESIA
Autoridad española de supervisión de la IA

Qué es la nueva Ley de IA en España

España aprobó el 26 de mayo de 2026 el Proyecto de Ley Orgánica para el buen uso y la gobernanza de la IA. No nace de cero, sino que traslada al ordenamiento español el Reglamento (UE) 2024/1689 (conocido como AI Act) y concreta quién lo supervisa, cómo se sancionan los incumplimientos y mediante qué procedimientos.

Una norma que ejecuta el Reglamento Europeo

El AI Act es directamente aplicable en toda la Unión desde agosto de 2024 y su régimen sancionador es plenamente exigible desde el 2 de agosto de 2026. La ley española se encarga de su gobernanza y ejecución. Nombra a la AESIA como autoridad nacional, reparte competencias con la AEPD y los supervisores sectoriales y precisa cómo se sancionan las infracciones.

La norma trabaja por niveles de riesgo. Cuanto mayor es el impacto de un sistema sobre la seguridad o los derechos de las personas, más obligaciones acumula. No prohíbe usar IA en la empresa, sino que establece cómo hacerlo con garantías.

La norma de un vistazo

Norma

Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial.

Estado

Aprobada en Consejo de Ministros el 26 de mayo de 2026 y en tramitación parlamentaria por vía de urgencia.

Plena aplicación del régimen sancionador

2 de agosto de 2026, conforme al Reglamento (UE) 2024/1689.

Autoridad supervisora

La AESIA como autoridad nacional, junto con la AEPD y los supervisores sectoriales en sus ámbitos.

Ámbito

Toda empresa cuyos sistemas de IA produzcan efectos en España o la UE, sin importar su tamaño.

CALENDARIO DE APLICACIÓN DEL AI ACT

Ago 2024
El AI Act entra en vigor

›

Feb 2025
Prácticas prohibidas y alfabetización

›

Ago 2025
Modelos de propósito general

›

Ago 2026
Alto riesgo y aplicación plena en España

›

Ago 2027
Alto riesgo en productos regulados

Las prohibiciones ya son exigibles desde febrero de 2025. El grueso de obligaciones de alto riesgo y la aplicación plena del régimen sancionador llegan el 2 de agosto de 2026.

A quién afecta y los cuatro niveles de riesgo

La ley alcanza a cualquier empresa que desarrolle, comercialice o use sistemas de IA con efectos en España o la UE. Las obligaciones no dependen del tamaño de la organización, sino del nivel de riesgo de cada sistema. Usos tan habituales como la IA en selección de personal, el scoring crediticio, la atención al cliente o la generación de contenido pueden acarrear obligaciones nuevas.

CLASIFICACIÓN POR NIVEL DE RIESGO DEL AI ACT

PROHIBIDO **Riesgo inaceptable**

Hay diez prácticas vetadas que ninguna empresa puede usar, como las técnicas subliminales dañinas, la explotación de vulnerabilidades, la categorización biométrica sensible, el social scoring o el reconocimiento de emociones en el trabajo y la educación, a las que España ha sumado los deepfakes sexuales.

ALTO RIESGO **Obligaciones reforzadas**

IA en selección de personal, educación, crédito, biometría, servicios esenciales o componentes de seguridad de productos. Exige gestión de riesgos, documentación técnica, supervisión humana, registro y evaluación de conformidad.

RIESGO LIMITADO **Transparencia**

Sistemas que interactúan con personas o generan contenido. Se obliga a informar de que se está ante una IA (p. ej. un chatbot) y a etiquetar el contenido sintético de forma legible y detectable por máquinas.

RIESGO MÍNIMO **Buenas prácticas**

La gran mayoría de usos (asistentes, filtros, productividad). Sin obligaciones específicas, más allá de las medidas voluntarias y la alfabetización en IA del personal.

Lo primero es saber dónde encaja cada sistema

El error más común no es incumplir una obligación concreta, sino no haber clasificado los sistemas. Sin un inventario y una clasificación por riesgo, una empresa no sabe qué obligaciones le aplican ni puede demostrar diligencia ante la AESIA. La clasificación es el punto de partida de todo el cumplimiento.

Cómo encajan los usos más comunes

ALTO **Personas y acceso a servicios**

Selección y evaluación de personal, scoring crediticio, biometría de acceso o IA dentro de un componente de seguridad de un producto.

LIMITADO **Trato con el público**

Chatbots de atención y generadores de texto o imagen de cara al cliente, siempre con aviso y etiquetado.

MÍNIMO **Uso interno**

Copilotos de productividad, filtros antispam o asistentes de redacción sin efecto sobre derechos.

PROHIBIDO **Líneas que no se cruzan**

Social scoring, categorización biométrica sensible o reconocimiento de emociones en el trabajo.

El coste de no cumplir

Las infracciones se clasifican en muy graves, graves y leves, con un tope que crece según la gravedad. La ley aplica criterios de proporcionalidad y da un trato específico a pymes y startups. Hay reducciones por pronto pago o por adoptar medidas correctoras, pero el riesgo no es solo económico.

35 M€
o el 7 % de la facturación anual mundial (muy grave)

15 M€
o el 3 % de la facturación (grave)

2 ago 26
desde cuándo es exigible el régimen

MUY GRAVE	**Uso de sistemas de IA prohibidos**	Hasta 35 M€ · 7 %
GRAVE	**Incumplir obligaciones de alto riesgo**	Hasta 15 M€ · 3 %
LEVE	**Infracciones formales o de transparencia**	Hasta 0,5 M€ · 0,5 %

Más allá de la multa

La sanción económica es la cara visible, pero el daño suele venir por otras vías que afectan a la continuidad del negocio.

- Prohibición o retirada del sistema, con paralización del servicio que dependía de él
- Daño reputacional y pérdida de confianza de clientes y socios
- Responsabilidad por decisiones automatizadas que afecten a derechos de las personas
- Bloqueo en concursos y contratos que ya exigen acreditar cumplimiento de IA

Proporcionalidad y atenuantes

Tamaño de la empresa

Se considera específicamente la situación de pymes y startups al graduar la sanción.

Pronto pago y corrección

Reducciones por pago anticipado o por adoptar medidas correctoras antes de la resolución.

Diligencia demostrable

El inventario, la clasificación y la trazabilidad documentados pesan a favor en una inspección, mientras que no tenerlos pesa en contra.

Las ocho obligaciones de cumplimiento

Este es el trabajo de fondo que la ley exige a las empresas con sistemas de IA en uso. La intensidad de cada obligación depende del nivel de riesgo del sistema, pero el conjunto define la diligencia que la AESIA esperará poder verificar.

TODOS **Inventario de sistemas de IA**
Identificar todos los sistemas y agentes de IA en uso, incluido el shadow AI que no figura en el inventario oficial.

TODOS **Clasificación por nivel de riesgo**
Asignar cada sistema a una de las cuatro categorías del AI Act, desde prohibido hasta riesgo mínimo.

ALTO RIESGO **Supervisión humana efectiva**
Garantizar control humano sobre las decisiones que afecten a la seguridad o a los derechos fundamentales.

LIMITADO **Transparencia y explicabilidad**
Informar cuando una persona interactúa con IA y poder explicar cómo y por qué decide el sistema.

ALTO RIESGO **Documentación técnica y registro**
Mantener la documentación de conformidad y registrar los sistemas de alto riesgo donde sea exigible.

ALTO RIESGO **Evaluación de impacto en derechos**
Evaluar el impacto sobre los derechos fundamentales antes de poner en marcha sistemas de alto riesgo.

GENERATIVA **Etiquetado del contenido con IA**
Marcar de forma legible y detectable por máquinas el contenido sintético, ya sea imagen, audio, vídeo o texto.

ORGANIZACIÓN **Formación y alfabetización en IA**
Asegurar que el personal que opera o se ve afectado por la IA cuenta con la formación adecuada.

Qué tendrás que poder enseñar

El cumplimiento se demuestra con un expediente. Ante una inspección, la AESIA esperará encontrar la documentación que respalda cada sistema de alto riesgo.

- Inventario y clasificación de todos los sistemas de IA
- Documentación técnica de los sistemas de alto riesgo
- Evaluación de impacto en los derechos fundamentales
- Registro de actividad y trazas de auditoría con su retención
- Constancia de la supervisión humana y de la formación del personal

Dónde fallan las empresas y cómo evitarlo

La mayoría de los incumplimientos no nacen de una mala intención, sino de puntos ciegos. Suele tratarse de actividad de IA que nadie registró, de decisiones automatizadas que nadie revisa o de trazas que no existen cuando el supervisor las reclama. Estos son los fallos más frecuentes y la forma de cerrarlos.

PUNTO CIEGO **Shadow AI sin inventariar**

Empleados usando ChatGPT, Copilot o Claude por su cuenta. Si no aparece en el inventario, no se puede clasificar ni gobernar.

- Descubrir el uso real en el egress de red y el navegador, atribuido a persona y equipo.

ALTO RIESGO **IA en RRHH sin supervisión**

Cribado de currículums o evaluación de personal con IA suele ser de alto riesgo y exige control humano y trazabilidad.

- Marcar estos sistemas como alto riesgo e imponer revisión humana antes de decidir.

AUDITORÍA **Sin trazabilidad de las decisiones**

Cuando la AESIA pregunte qué hizo un sistema y por qué, hará falta un registro íntegro, porque reconstruirlo a posteriori no vale.

- Registrar cada petición con trazas estructuradas y retención adecuada desde el día uno.

TRANSPARENCIA **Contenido generado sin etiquetar**

Imágenes, vídeos o textos creados con IA publicados sin marca de agua ni aviso al usuario incumplen la transparencia.

- Etiquetar el contenido sintético y avisar de que se interactúa con una IA.

CADENA DE IA **Proveedores y terceros**

Usas IA de un proveedor, pero el uso y sus efectos siguen siendo responsabilidad tuya ante la AESIA.

- Exigir al proveedor la documentación de conformidad y registrar qué hace en tu contexto.

ORGANIZACIÓN **Un equipo sin formación**

Si el personal no sabe qué puede o no puede hacer con la IA, los incidentes llegan solos.

- Un plan de alfabetización en IA y una política de uso claras para toda la plantilla.

De cada obligación a una capacidad operativa

RenLayer es un plano de control de gobernanza y observabilidad de IA. Se sitúa delante de cada llamada a un modelo, de forma que basta con redirigir esas llamadas hacia RenLayer para gobernarlas, sin instalar SDKs ni librerías y sin reescribir la lógica de las aplicaciones. Así convierte las obligaciones de la ley en controles que se pueden activar, medir y demostrar.

Obligación → capacidad

Inventario y shadow AI → Shadow AI
Descubre cada modelo, agente y herramienta en uso, atribuido a persona y departamento.

Clasificación por riesgo → Activity Graph
Mapea qué sistemas tocan qué datos y servicios para clasificarlos por nivel de riesgo.

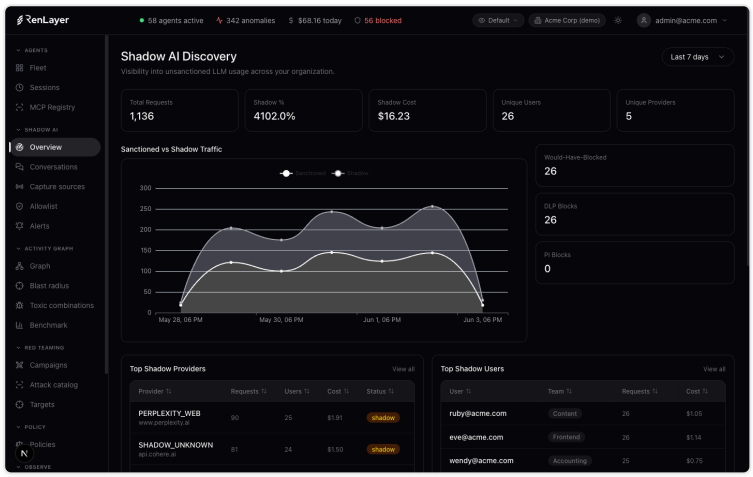
Transparencia y control → Policy
Aplica políticas en tiempo real, como bloquear una petición, redactar datos personales o fijar reglas por sistema.

Trazabilidad y supervisión → Observe
Registra cada petición con trazas de auditoría estructuradas, exportables al SIEM.

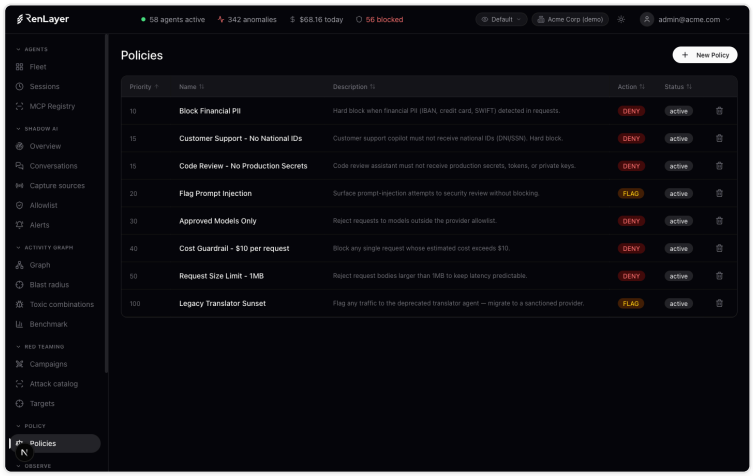
Evaluación de riesgos → Red Teaming
Detecta inyección de instrucciones, fugas y comportamientos de riesgo antes de producción.

Supervisión humana → Admin
Centraliza identidades de agentes, permisos y el control humano de todos los sistemas de IA.

Clasificación frente al AI Act → AI Act Review
Clasifica cada agente frente a la ley, con la justificación referida al artículo y un texto de remediación por cada brecha.



SHADOW AI Inventario del uso real de IA, atribuido a persona, equipo y departamento.



POLICY Reglas que permiten, bloquean o marcan una petición antes de llegar al proveedor.

Clasifica cada agente frente a la ley y corrige sus brechas

Cada agente de IA puede clasificarse frente a la ley sin trabajo manual. RenLayer parte del repositorio del agente, una descripción funcional y un cuestionario guiado. Con eso devuelve un estudio de riesgo con el nivel que le corresponde, la justificación referida al artículo, la lista de obligaciones y las brechas detectadas. Para cada obligación y cada brecha genera además un texto listo para pegar en tu sistema de gestión.

Conectar
El repositorio del agente

›

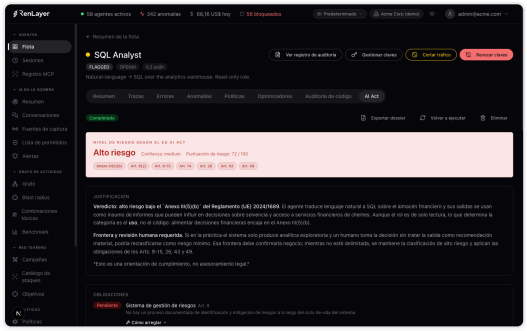
Describir
Función y cuestionario guiado

›

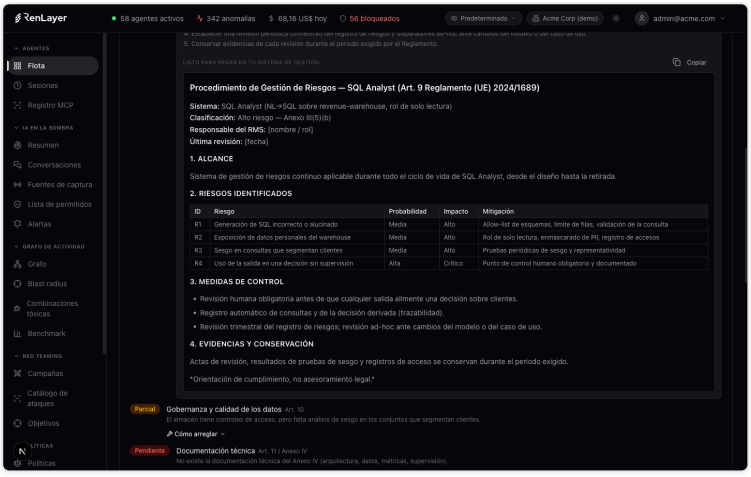
Clasificar
Nivel, justificación y obligaciones

›

Remediar
Texto para tu sistema de gestión



CLASIFICACIÓN Nivel de riesgo, justificación citando el Anexo o el artículo, obligaciones y brechas del agente.



CÓMO ARREGLAR Por cada obligación, un procedimiento listo para copiar y pegar en tu sistema de gestión.

Del diagnóstico abierto al expediente completo

Ver el nivel de riesgo de un agente y su justificación está abierto a cualquiera, para que puedas situar a tus agentes frente a la ley desde el primer momento. El expediente completo, con la lista de obligaciones, las brechas, el informe exportable a PDF y los textos de remediación, se incluye en los planes superiores.

Hoja de ruta antes del 2 de agosto de 2026

Llegar a tiempo no requiere un gran proyecto, sino un proceso ordenado en cinco pasos. Los dos primeros, que son los que más cuesta arrancar, se pueden cubrir en días con una evaluación de cumplimiento.

Inventariar — Toda la IA en uso, incluido el shadow AI

›

Clasificar — Por nivel de riesgo del AI Act

›

Controlar — Supervisión, políticas y trazas

›

Documentar — Conformidad y registro

›

Evaluar — Impacto en derechos

Qué hacer en cada paso

- Inventariar el uso real de IA en la red y el navegador, atribuido a personas.
- Clasificar cada sistema entre prohibido, alto, limitado o mínimo.
- Controlar con supervisión humana, políticas de bloqueo y registro de auditoría.
- Documentar la parte técnica y registrar los sistemas de alto riesgo.
- Evaluar el impacto en derechos allí donde sea exigible.

Acelera los dos primeros pasos

En días y sin reescribir tus aplicaciones, una evaluación de cumplimiento de RenLayer entrega el inventario de tu IA, su clasificación por riesgo y un informe de brechas priorizado. Se despliega en modo observación, sin impacto en producción.

- Inventario y clasificación en menos de una semana
- Informe de brechas priorizado frente a la ley
- Integración en menos de 24 horas, en modo solo lectura

Si vas justo de tiempo, prioriza

No todo pesa igual de cara al 2 de agosto. Empieza por lo que más te expone a una sanción y por lo que más tarda en estar listo.

- Identifica primero el shadow AI y los sistemas de alto riesgo
- Activa la supervisión humana donde haya decisiones sobre personas
- Empieza ya a registrar las trazas, porque lo que no se registra no se recupera
- Aborda la documentación formal cuando los controles ya funcionen

CÓMO EMPEZAR

Evalúa tu exposición antes de agosto de 2026.

Del primer diagnóstico al cumplimiento demostrable, en tres pasos. Sin reescribir tus aplicaciones y sin interrumpir el tráfico.

PASO 01

Evaluación gratuita

Inventario de tu IA y clasificación por nivel de riesgo en días, desplegada en modo observación.

PASO 02

Informe de brechas

Lista priorizada de obligaciones pendientes y de los riesgos de sanción más urgentes.

PASO 03

Plan de cumplimiento

Controles activos, supervisión humana y trazabilidad completa para demostrar el cumplimiento ante el supervisor.

Pon tu IA en regla antes del 2 de agosto de 2026

Solicita una evaluación de cumplimiento de la Ley de IA y recibe el inventario de tu IA, su clasificación por riesgo y un informe de brechas priorizado, sin impacto en producción.

Solicitar evaluación · renlayer.com/es/ley-ia-espana

Respondemos en menos de 24 horas laborables · hola@renlayer.com

Documento de carácter divulgativo, no constituye asesoramiento jurídico. La norma se encuentra en tramitación parlamentaria y su redacción puede variar. Fuentes: Gobierno de España (MTDFP, nota de prensa del 26/05/2026) y Reglamento (UE) 2024/1689.