INFORME COMPLETO

La Nueva Ley de Inteligencia Artificial en España

Régimen sancionador, plazos, obligaciones y hoja de ruta para empresas

Aprobado en Consejo de Ministros	Multas de hasta	Supervisora:
26 Mayo 2026	**35 millones** o 7% facturación global	**AESIA** Sede en A Coruña

Mayo 2026 · Uso confidencial

1. Contexto: qué había antes y por qué llega esta ley

1.1 El punto de partida: el AI Act europeo

España no legisla en el vacío. El marco de referencia es el Reglamento (UE) 2024/1689, conocido como AI Act, aprobado por el Parlamento Europeo y el Consejo de la UE en 2024. Es el primer gran cuerpo normativo del mundo dedicado específicamente a regular la inteligencia artificial. Al ser un reglamento europeo, es directamente aplicable en todos los estados miembros sin necesidad de transposición formal, lo que significa que sus obligaciones ya vinculan a las empresas españolas independientemente de que exista o no una ley nacional.

El AI Act adopta un enfoque basado en el riesgo, dividiendo los sistemas de IA en cuatro categorías:

- Riesgo inaceptable: prohibidos directamente (manipulación subliminal, puntuación social, reconocimiento biométrico masivo en tiempo real en espacios públicos).
- Riesgo alto: permitidos pero con obligaciones estrictas de documentación, supervisión humana y registro (selección de personal, educación, crédito, infraestructura crítica).
- Riesgo limitado: obligaciones de transparencia (chatbots, deepfakes, generación de contenido).
- Riesgo mínimo: sin obligaciones específicas (filtros de spam, videojuegos con IA).

1.2 Calendario de aplicación del AI Act (ya vigente)

El AI Act no entró en vigor de golpe. Siguió un calendario escalonado que ya ha arrancado:

Fecha	Qué entra en vigor
1 agosto 2024	Entrada en vigor del Reglamento. Las empresas deben empezar a prepararse.
2 febrero 2025	Prácticas prohibidas (riesgo inaceptable) ya son ilegales. Obligación de alfabetización en IA para el personal (Art. 4).
2 agosto 2025	Reglas de gobernanza y obligaciones para modelos de IA de propósito general (GPAI como GPT-4, Gemini, Claude).
2 agosto 2026	Plena aplicación para sistemas de alto riesgo del Anexo III (RRHH, educación, crédito, biometría). Etiquetado obligatorio de contenido generado por IA.
2 agosto 2027	Sistemas de alto riesgo integrados en productos regulados (dispositivos médicos, maquinaria, vehículos).
Diciembre 2027	Fecha límite objetivo para que la ley española esté aprobada por el Parlamento.

1.3 Qué existía en España antes del 26 de mayo de 2026

Antes de que el Consejo de Ministros aprobara el proyecto de ley, España ya tenía cierta infraestructura:

- La AESIA (Agencia Española de Supervisión de la Inteligencia Artificial) fue creada en 2023, siendo España uno de los primeros países europeos en designar su autoridad nacional de supervisión. Tiene sede en A Coruña y en 2025-2026 publicó 16 guías de cumplimiento no vinculantes.
- El AI Act europeo ya era aplicable de forma directa, por lo que las prohibiciones de riesgo inaceptable llevan vigentes desde febrero de 2025.
- La AEPD (Agencia Española de Protección de Datos) venía ya sancionando usos de IA que vulneraban el RGPD, con un incremento del 340% en investigaciones relacionadas con IA en 2025 respecto a 2024.
- El Gobierno aprobó un primer anteproyecto de ley en marzo de 2025 y abrió un período de alegaciones públicas, durante el cual el texto fue revisado por el Consejo General del Poder Judicial y otras instituciones.
- España activó el primer sandbox regulatorio de IA de la UE, permitiendo que empresas puedan testar sistemas de IA innovadores bajo supervisión directa de AESIA sin riesgo de sanciones.

Dato clave para empresas

El AI Act ya es derecho vigente en España. Que la ley nacional esté en tramitación parlamentaria NO exime del cumplimiento del reglamento europeo. Las obligaciones del Artículo 4 (alfabetización en IA) están en vigor desde agosto de 2025, y las de alto riesgo desde agosto de 2026.

2. Las novedades del proyecto de ley español (26 mayo 2026)

El Consejo de Ministros aprobó el 26 de mayo de 2026 el Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial. El texto, elaborado por el Ministerio para la Transformación Digital y de la Función Pública liderado por Óscar López, añade al marco europeo un conjunto de especificidades nacionales. Estas son las principales novedades:

2.1 Un régimen sancionador propio y más detallado

Aunque el AI Act ya prevé sanciones, necesita de una ley nacional que las concrete, designe al organismo competente para imponerlas y establezca el procedimiento. El proyecto de ley español hace exactamente eso, con un desglose de tres tramos:

Tipo de infracción	Cuantía	Ejemplos de conductas
Muy grave (prácticas prohibidas)	Hasta 35M€ o 7% facturación mundial (lo que sea mayor)	Comercializar o desplegar un sistema de IA expresamente prohibido. Deepfakes sexuales sin consentimiento.
Muy grave (alto riesgo)	Hasta 15M€ o 3% facturación mundial	Sistemas de alto riesgo sin supervisión humana, sin documentación o sin registro en la base de datos de la UE.
Grave	Entre 500.001€ y 7,5M€	Incumplimientos de obligaciones de transparencia, accesibilidad, gestión de riesgos o auditoría en sistemas de alto riesgo.
Leve	De 6.000€ a 500.000€ (o 0,5% facturación)	No cooperar con la AESIA, falta de etiquetado de contenido generado por IA, incumplimientos formales.

Para pymes y empresas emergentes, el reglamento europeo permite aplicar la cuantía menor entre el importe fijo y el porcentaje sobre facturación, para evitar sanciones desproporcionadas. Además de multas económicas, se prevén medidas como la retirada del mercado, desconexión o prohibición de un sistema cuando haya provocado un incidente grave o suponga un riesgo inaceptable.

2.2 La prohibición expresa de deepfakes sexuales (iniciativa española)

Esta es quizás la novedad más mediática y una de las que España puede reclamar como propia. El Gobierno español impulsó en el debate europeo una enmienda específica para prohibir la comercialización y el uso de sistemas de IA capaces de generar o manipular imágenes, vídeos o audios realistas de contenido sexual sin el consentimiento de las personas representadas. Bruselas acabó respaldando esa propuesta, que queda reforzada ahora en la ley nacional. La medida responde directamente a la polémica por la difusión de

desnudos falsos de mujeres y menores generados con herramientas de IA, y su sanción está en el tramo más alto del régimen sancionador.

2.3 Obligación de etiquetado de contenido generado por IA

La ley refuerza y concreta las obligaciones de transparencia del AI Act respecto a los contenidos artificialmente generados. Cualquier imagen, audio, vídeo o texto creado o manipulado sustancialmente con IA deberá llevar una etiqueta o identificación clara que permita a los ciudadanos saber que no es de origen humano. Esto afecta especialmente a medios de comunicación, agencias de publicidad, plataformas de contenido y herramientas de generación de imágenes y texto. La obligación de etiquetado entra en vigor el 2 de agosto de 2026, con independencia de que la ley nacional haya completado su tramitación parlamentaria.

2.4 Protección reforzada de menores y vulnerables

La ley española amplía la protección de colectivos vulnerables más allá de lo que establece el reglamento europeo. Quedan expresamente prohibidos:

- Juguetes inteligentes o aplicaciones dirigidas a menores que puedan incitarles a realizar retos peligrosos o fomentar comportamientos adictivos o dañinos.
- Sistemas de IA que aprovechen vulnerabilidades psicológicas de usuarios con adicciones (ej: chatbots que detecten compulsión al juego y empujen a apostar más).
- Cualquier sistema que explote vulnerabilidades de personas mayores o con discapacidad para manipular su comportamiento o decisiones.

2.5 Centralización de la gobernanza en la AESIA

La ley ordena la arquitectura de supervisión en España. La AESIA, dirigida por Alberto Gago con sede en A Coruña, se convierte en el organismo central. El texto prevé que cuente con 50 analistas antes de que acabe 2026. Sus competencias incluyen:

- Supervisar el cumplimiento del AI Act y de la ley nacional en el territorio español.
- Investigar incidentes y reclamaciones, incluso las presentadas de forma anónima por ciudadanos.
- Coordinar con la AEPD (protección de datos), el Banco de España, la CNMV y otros reguladores sectoriales.
- Imponer sanciones y ordenar medidas correctoras, incluyendo la retirada del mercado de sistemas de IA.
- Gestionar el sandbox regulatorio para que empresas puedan testar sus sistemas sin riesgo de sanción.

2.6 El gran debate: las administraciones públicas quedan exentas de multas

Uno de los puntos más criticados y debatidos durante la fase de consultas públicas es que el texto excluye al sector público del régimen de multas económicas. Cuando una administración pública cometa una infracción, la respuesta será únicamente una resolución

declarando el incumplimiento, acompañada de un apercibimiento y medidas correctoras. También podrán abrirse actuaciones disciplinarias, pero no se impondrán multas administrativas como las previstas para el sector privado.

El doble rasero criticado

Si la policía, un ministerio o una comunidad autónoma utiliza un sistema de reconocimiento biométrico masivo en tiempo real prohibido por el AI Act, la consecuencia es una amonestación. Si una empresa privada hace exactamente lo mismo, enfrenta una multa de hasta 35 millones de euros. Múltiples organizaciones de defensa de derechos digitales han señalado que esto genera un incentivo perverso y debilita la protección de los ciudadanos frente al Estado.

2.7 Nuevas obligaciones para el sector público

A cambio de la exención de multas, el texto incorpora medidas específicas para impulsar el buen uso de la IA en el sector público, introducidas tras las sugerencias recibidas durante el período de alegaciones. Aunque los detalles completos aún se conocerán durante la tramitación parlamentaria, incluyen obligaciones de inventariar los sistemas de IA utilizados, garantizar supervisión humana en decisiones que afecten a derechos fundamentales y publicar información sobre los algoritmos empleados en decisiones administrativas.

3. ¿Cuándo habrá las primeras multas?

Esta es la pregunta más práctica para cualquier empresa o directivo. La respuesta requiere distinguir entre el marco europeo (ya vigente) y la ley española (en tramitación).

3.1 Las multas europeas: ya se pueden imponer

El AI Act es directamente aplicable en España desde sus respectivas fechas de entrada en vigor. Las prohibiciones de riesgo inaceptable llevan vigentes desde febrero de 2025. Las obligaciones de alto riesgo y el etiquetado de contenido IA entran en vigor el 2 de agosto de 2026. Técnicamente, la AESIA ya tiene base jurídica para actuar bajo el reglamento europeo.

Sin embargo, la AESIA ha indicado públicamente que priorizará la acción educativa y de acompañamiento durante los primeros meses de aplicación plena (aproximadamente hasta finales de 2026), con un enfoque pedagógico antes que punitivo. Después de ese período se espera una aplicación más estricta.

3.2 Las multas de la ley española: pendientes del Parlamento

El proyecto de ley aprobado en Consejo de Ministros el 26 de mayo de 2026 debe ahora completar su tramitación parlamentaria en el Congreso y el Senado. El objetivo del Gobierno es obtener la aprobación definitiva antes de diciembre de 2027. Esto significa que durante más de un año existirán obligaciones vigentes por vía europea, pero sin la capacidad sancionadora plena que prevé la ley nacional.

> **Ventana de riesgo inmediato**
> No esperes a que la ley española esté aprobada. El RGPD ya permite a la AEPD sancionar usos de IA que vulneren protección de datos, privacidad, biometría o decisiones automatizadas. La AEPD abrió 147 investigaciones relacionadas con IA en 2025, un 340% más que en 2024. Y la AESIA ya tiene 23 investigaciones preliminares abiertas.

3.3 Línea temporal de riesgo sancionador

Período	Situación de riesgo sancionador
Ya (desde feb. 2025)	PROHIBICIONES en vigor. Usar IA para manipulación, puntuación social o clasificación biométrica masiva es ilegal ya. Riesgo de sanción vía AESIA + AEPD.
2 agosto 2026	Obligaciones de alto riesgo y etiquetado IA en vigor. Sistema plenamente sancionable por el AI Act europeo.
2026-2027 (estimado)	Fase educativa de la AESIA. Primeras investigaciones formales. Primeras multas posiblemente a empresas con incumplimientos graves o flagrantes.

Fin 2027 (estimado)	Aprobación de la ley española. Régimen sancionador nacional plenamente operativo. Multas de hasta 35M€ aplicables por AESIA.
2028 en adelante	Madurez regulatoria. Supervisión sistemática. Multas rutinarias por incumplimientos de cualquier tipo.

4. Por qué motivos puede multarte: el catálogo completo de infracciones

Conocer exactamente qué conductas son sancionables es el primer paso para cualquier estrategia de compliance. El catálogo se divide en conductas prohibidas (riesgo inaceptable, las más graves) y obligaciones incumplidas (riesgo alto y limitado).

4.1 Infracciones muy graves: prácticas prohibidas (hasta 35M€ o 7%)

Son las conductas que el AI Act y la ley española prohíben de forma absoluta, sin excepciones. Comercializarlas, desplegarlas o usarlas deliberadamente conlleva las sanciones máximas:

- Manipulación subliminal o engañosa: usar técnicas por debajo del umbral de conciencia o deliberadamente engañosas para alterar el comportamiento de una persona causándole perjuicio.
- Explotación de vulnerabilidades: aprovecharse de la edad, discapacidad, situación económica o social precaria para influir en el comportamiento de personas o grupos de manera dañina.
- Sistemas de puntuación social (social scoring): evaluar a personas en base a su comportamiento, características o condición social para tomar decisiones sobre su acceso a servicios, oportunidades o derechos. Esto incluye sistemas de crédito social.
- Reconocimiento biométrico masivo en tiempo real en espacios públicos: salvo excepciones muy tasadas para la seguridad nacional (con autorización judicial previa).
- Clasificación biométrica por categorías sensibles: sistemas que infieran la raza, ideología política, religión, orientación sexual o estado de salud a partir de datos biométricos.
- Deepfakes sexuales sin consentimiento: crear o difundir imágenes, vídeos o audios de contenido sexual de personas reales generados con IA sin su consentimiento explícito.
- Material de abuso sexual infantil generado por IA: creación de pornografía infantil mediante herramientas de inteligencia artificial.
- Sistemas que induzcan comportamientos peligrosos en menores: juguetes o aplicaciones que inciten a retos peligrosos, conductas adictivas o dañinas.
- Sistemas que exploten adicciones: chatbots o aplicaciones que detecten vulnerabilidades psicológicas (adicción al juego, compras compulsivas) y las aprovechen para obtener un beneficio comercial.

4.2 Infracciones muy graves: sistemas de alto riesgo sin cumplir (hasta 15M€ o 3%)

Los sistemas de alto riesgo están enumerados en el Anexo III del AI Act. Las principales categorías que afectan a empresas españolas incluyen:

- Sistemas de selección y evaluación de personal: herramientas de IA para cribado de CVs, evaluación de candidatos o gestión del desempeño de empleados.
- Sistemas de acceso a educación y formación: plataformas adaptativas de aprendizaje, evaluación automática de exámenes, sistemas de admisión.
- Sistemas de acceso a servicios financieros esenciales: scoring crediticio, evaluación de solvencia, detección de fraude con decisiones automatizadas.
- Sistemas de gestión de infraestructuras críticas: energía, agua, transporte, redes de comunicación.
- Sistemas de atención sanitaria: diagnóstico médico asistido por IA, priorización de pacientes, robots quirúrgicos.
- Sistemas relacionados con la aplicación de la ley (solo para administraciones): análisis de riesgo de reincidencia, poligrafía, análisis de material probatorio.
- Sistemas de control de fronteras y migración (solo para administraciones).

Para cualquiera de estos sistemas, las infracciones sancionables con hasta 15M€ o 3% de facturación incluyen: no llevar la documentación técnica exigida, no registrar el sistema en la base de datos pública de la UE, no realizar la Evaluación de Impacto en Derechos Fundamentales (EIDF), no implementar supervisión humana significativa, no garantizar la trazabilidad y auditoría del sistema, o poner el sistema en servicio sin haber obtenido la conformidad CE si aplica.

4.3 Infracciones graves: incumplimientos de transparencia y gobernanza (hasta 7,5M€)

- No etiquetar contenido generado por IA (imágenes, audio, vídeo, texto) cuando sea obligatorio.
- No informar a los usuarios de que están interactuando con un sistema de IA (ej: chatbot que no se identifica como tal).
- Proveedores de modelos GPAI (modelos de propósito general) que no cumplan con las obligaciones de transparencia hacia la AI Office.
- No mantener los registros de incidentes o no notificar incidentes graves a la AESIA.
- No tener una política de IA documentada o no designar un responsable de cumplimiento cuando sea exigible.

4.4 Infracciones leves (desde 6.000€)

- No cooperar con la AESIA durante una inspección o investigación.
- Incumplimientos formales de documentación sin impacto directo en derechos de las personas.
- No haber completado la formación en alfabetización en IA para el personal que usa o desarrolla sistemas de IA (Artículo 4 del AI Act, obligatorio desde agosto 2025).
- No tener un inventario interno de los sistemas de IA utilizados.

5. Cómo protegerse: hoja de ruta completa para empresas

El cumplimiento regulatorio de IA no es un proyecto tecnológico. Es un proyecto de gobernanza que requiere orden, documentación y formación. Una PYME puede alcanzar un nivel aceptable de cumplimiento en 8-12 semanas de trabajo estructurado. Aquí está la hoja de ruta completa.

5.1 Paso 1: Inventario y clasificación de sistemas de IA

Antes de hacer nada, necesitas saber qué tienes. El 68% de las empresas españolas todavía no ha realizado una Evaluación de Impacto para sus sistemas de IA, y más de la mitad no tiene ni siquiera un inventario. Sin inventario, no puedes cumplir.

Qué incluir en el inventario

- Nombre y descripción del sistema de IA.
- Proveedor (interno o externo) y versión.
- Finalidad y casos de uso concretos en tu empresa.
- Datos personales que procesa y base jurídica RGPD.
- Clasificación de riesgo según el AI Act (mínimo, limitado, alto, inaceptable).
- Responsable interno del sistema.
- Estado de cumplimiento y brechas identificadas.

> **Herramienta práctica**
> La AESIA ofrece consultas gratuitas a través de su portal web para ayudar a clasificar sistemas. El plazo medio de respuesta es de 15 días hábiles. Para sistemas con clasificación dudosa, es recomendable documentar el proceso de razonamiento seguido para llegar a la clasificación.

5.2 Paso 2: Gobernanza y estructura organizativa

El AI Act requiere que las organizaciones tengan estructuras claras de responsabilidad para la IA. Esto implica:

Política de IA

Un documento de 1-5 páginas que defina los principios de uso de IA en tu organización, su alcance, las responsabilidades de cada área y los procesos de aprobación para nuevos sistemas. No necesita ser complejo, pero debe existir y estar firmado por la dirección.

Designar un Responsable de IA (AI Officer)

Para empresas que usen sistemas de alto riesgo, es imprescindible designar una persona responsable del cumplimiento de IA. En empresas medianas puede ser el DPO existente

con funciones ampliadas. En empresas grandes, debería ser un rol dedicado o incluso un comité de IA. Este responsable debe tener formación específica en el AI Act y la ley española.

Coordinación con el DPO

El AI Act y el RGPD se solapan en muchos puntos, especialmente en sistemas que procesan datos personales. La AEPD y el Comité Europeo de Protección de Datos han indicado que la Evaluación de Impacto relativa a la Protección de Datos (EIPD) de un sistema de IA de alto riesgo debe integrarse con la evaluación de conformidad del AI Act. El DPO debe estar involucrado desde el inicio.

5.3 Paso 3: Auditorías de IA

La auditoría es el mecanismo central de demostración de cumplimiento. La AESIA puede solicitar informes de auditoría en cualquier momento. Existen dos niveles:

Auditoría interna

Una revisión anual mínima de todos los sistemas de IA del inventario, documentando su estado de cumplimiento, los riesgos identificados y las medidas correctoras aplicadas. Para sistemas de alto riesgo, se recomienda una revisión semestral. Debe generar un informe escrito que quede archivado.

Auditoría externa

Para sistemas de alto riesgo y para organizaciones que quieran demostrar un cumplimiento sólido ante clientes, inversores o la AESIA, una auditoría externa por un tercero independiente es la mejor protección. El mercado de servicios especializados en España está madurando:

- Las Big Four (Deloitte, PwC, EY, KPMG) ya ofrecen servicios especializados de auditoría de IA, con tarifas a partir de 15.000 euros.
- Consultoras boutique como Sngular o Enzyme Advising Group ofrecen precios más competitivos para PYMEs, desde 8.000 euros por sistema.
- Para una empresa mediana con 3-5 sistemas de IA, el coste total de una auditoría externa completa oscila entre 25.000 y 80.000 euros anuales según complejidad.

5.4 Paso 4: Evaluación de Impacto en Derechos Fundamentales (EIDF)

Obligatoria para todos los sistemas de alto riesgo antes de su puesta en servicio. Debe incluir:

- Descripción detallada del sistema, sus datos de entrenamiento y su lógica de funcionamiento.
- Identificación de los derechos fundamentales que podrían verse afectados (privacidad, no discriminación, presunción de inocencia, etc.).
- Evaluación de los riesgos de sesgo, error y abuso.

- Medidas de mitigación implementadas.
- Plan de monitoreo continuo y criterios para revisar o retirar el sistema.
- Evidencia de supervisión humana significativa: qué decide el humano, cómo puede anular la decisión de la IA, con qué frecuencia revisa los resultados.

5.5 Paso 5: Formación y alfabetización en IA (obligatoria desde agosto 2025)

El Artículo 4 del AI Act exige que las organizaciones garanticen que el personal que trabaja con sistemas de IA tiene un nivel de alfabetización IA suficiente para entender los riesgos y limitaciones de estas tecnologías. El incumplimiento puede acarrear multas de hasta 15M€ o el 3% de facturación global.

- La formación debe estar documentada: evidencia del plan formativo, materiales utilizados, registros de asistencia y evaluaciones superadas.
- Debe adaptarse al rol: no es lo mismo el nivel exigible a un desarrollador que lo integra en sistemas que a un empleado de ventas que usa una herramienta de CRM con IA.
- Debe cubrir como mínimo: qué es la IA y qué no puede hacer, sesgos y alucinaciones, privacidad de datos al usar IA, cómo reconocer y escalar incidentes.
- Plataformas especializadas como Brain (startbrain.ai) ofrecen módulos adaptados por sector para documentar el cumplimiento del Artículo 4.

5.6 Paso 6: Registro en la base de datos pública de la UE

Los sistemas de IA de alto riesgo deben registrarse en la base de datos pública de la UE antes de su puesta en el mercado. El registro es gratuito y se realiza a través del portal de la AI Office de la Comisión Europea. Es un requisito formal pero con gran visibilidad: la AESIA puede verificarlo fácilmente y su ausencia es una infracción por sí sola.

5.7 Paso 7: Sellos de calidad y certificaciones

Aunque el AI Act no exige obligatoriamente una certificación ISO para cumplir, las normas técnicas son la forma más eficiente de estructurar el cumplimiento:

ISO 42001:2023 — Sistema de Gestión de IA

Es el estándar más relevante. Estructura exactamente el sistema de gestión que el AI Act exige documentar: política, roles, inventario, evaluación de riesgos, auditoría interna y ciclos de revisión. Adoptar ISO 42001 (con o sin certificación formal) facilita enormemente la respuesta a la AESIA en una eventual inspección. El coste de certificación oscila entre 8.000 y 30.000 euros según el alcance de la organización.

ISO 27001 — Seguridad de la información

Complementaria y frecuentemente ya implantada en empresas con madurez en gestión de datos. Cubre los aspectos de seguridad de los sistemas de IA (acceso, integridad, disponibilidad).

Marca de Confianza IA (en desarrollo)

La AESIA está trabajando en un esquema de certificación voluntaria para sistemas de IA que cumplan con el AI Act. Su existencia otorgará una ventaja competitiva a las empresas que la obtengan, especialmente en licitaciones públicas.

Certificación CE para alto riesgo integrado en productos

Los sistemas de IA de alto riesgo que formen parte de productos regulados (dispositivos médicos, maquinaria, vehículos) deben obtener el marcado CE antes de agosto de 2027.

5.8 Paso 8: Seguros de riesgo regulatorio de IA

El mercado asegurador está respondiendo a la nueva realidad regulatoria de la IA. Aunque el seguro no exime del cumplimiento ni evita la multa, puede cubrir los costes asociados:

- Seguro de responsabilidad civil por daños causados por sistemas de IA: cubre reclamaciones de terceros afectados por decisiones automatizadas erróneas o sesgadas.
- Seguro de defensa jurídica regulatoria: cubre honorarios legales, costes de representación ante la AESIA y gastos de investigación durante un procedimiento sancionador.
- Ciberseguro con cobertura de IA: algunos productos de ciberseguro ya incorporan cobertura específica para incidentes de seguridad en sistemas de IA.

Aseguradoras como AXA, Allianz, Zurich y Mapfre están desarrollando productos específicos para riesgo regulatorio de IA en España. El coste varía enormemente según la exposición de la empresa: para una PYME que use únicamente herramientas de terceros, las primas son relativamente asequibles (2.000-10.000€/año). Para empresas que desarrollen o desplieguen sistemas de alto riesgo, pueden superar los 50.000€ anuales.

> **Importante sobre los seguros**
> El seguro reduce el coste económico de un incidente regulatorio, pero no reduce la multa ni evita las medidas correctoras. Además, la mayoría de las pólizas excluyen explícitamente el pago de multas administrativas. Su valor principal es la cobertura de responsabilidad civil frente a terceros y los costes de defensa legal.

5.9 Paso 9: Sandbox regulatorio de la AESIA

España fue el primer país de la UE en activar un sandbox regulatorio de IA. Este entorno controlado permite a empresas, especialmente startups y PYMEs, testear sistemas de IA

innovadores bajo supervisión directa de la AESIA sin riesgo de sanciones durante el período de prueba. Es especialmente útil para:

- Empresas que desarrollan sistemas con clasificación de riesgo dudosa y quieren certeza jurídica antes de lanzar.
- Startups de alto riesgo (HR tech, edtech, fintech, healthtech) que necesitan validar su compliance antes de captar inversión.
- Empresas que quieren testear tecnología puntera sin la presión del régimen sancionador.

Las PYMEs tienen acceso prioritario a los sandboxes regulatorios que la AESIA tiene previsto poner en marcha a lo largo de 2026. La solicitud se tramita a través del portal web de la AESIA.

6. Checklist de cumplimiento: qué debe tener tu empresa antes de agosto 2026

Ante la AESIA, la clave es poder demostrar que has adoptado una actitud proactiva y diligente. Este checklist sintetiza las acciones prioritarias:

	Acción requerida	Prioridad
☐	Inventario documentado de todos los sistemas de IA utilizados (propios y de terceros)	URGENTE
☐	Clasificación de riesgo de cada sistema según el Anexo III del AI Act	URGENTE
☐	Formación en alfabetización IA documentada para todo el personal relevante (Art. 4)	URGENTE
☐	Política de IA corporativa aprobada por dirección	ALTA
☐	Responsable de IA (AI Officer) designado formalmente	ALTA
☐	Verificar que ningún sistema corresponde a práctica prohibida	URGENTE
☐	EIDF (Evaluación de Impacto en DDHH) para cada sistema de alto riesgo	ALTA
☐	Registro de sistemas de alto riesgo en la base de datos de la AI Office (UE)	ALTA
☐	Mecanismos de supervisión humana documentados para sistemas de alto riesgo	ALTA
☐	Etiquetado de contenido generado por IA en todos los canales (web, RRSS, publicidad)	2 agosto 2026
☐	Revisión de contratos con proveedores de IA para verificar sus obligaciones (Art. 25-27)	ALTA
☐	Coordinación con DPO para integrar AI Act y RGPD en las evaluaciones de impacto	MEDIA
☐	Auditoría interna del cumplimiento con informe documentado	MEDIA
☐	Considerar auditoría externa e ISO 42001 para sistemas de alto riesgo	MEDIA
☐	Evaluar seguro de responsabilidad civil y defensa jurídica IA	BAJA
☐	Monitorizar tramitación parlamentaria de la ley española y adaptar el compliance	CONTINUO

7. Sectores con mayor exposición regulatoria

No todas las empresas tienen el mismo nivel de exposición. Estos son los sectores donde el riesgo sancionador es mayor en España:

Sector	Principal exposición	Riesgo estimado

HR Tech / Recursos Humanos	Sistemas de selección y evaluación de personal (Anexo III). Todo el cribado de CVs con IA es alto riesgo.	MUY ALTO
Fintech / Banca	Scoring crediticio, evaluación de solvencia, detección de fraude automatizada.	MUY ALTO
Healthtech / Sanidad	Diagnóstico asistido por IA, triaje automático, gestión de listas de espera.	MUY ALTO
Edtech / Educación	Plataformas adaptativas, evaluación automática, sistemas de admisión.	ALTO
Marketing y Publicidad	Generación de contenido con IA, deepfakes publicitarios, segmentación hiperpersonalizada.	ALTO
Legal Tech	Análisis de contratos, predicción judicial, due diligence automatizada.	ALTO
Seguros	Pricing automatizado, evaluación de riesgo, gestión de siniestros con IA.	ALTO
E-commerce / Retail	Sistemas de recomendación, precios dinámicos, atención al cliente con IA.	MEDIO
Agencias de Marketing	Contenido generativo para clientes, chatbots sin identificación, deepfakes creativos.	MEDIO

8. Conclusiones y recomendaciones estratégicas

La aprobación del proyecto de ley el 26 de mayo de 2026 no marca el inicio de la regulación de la IA en España: marca su madurez. El AI Act europeo ya es derecho vigente, la AESIA ya tiene capacidad investigadora y la AEPD ya está sancionando. Lo que la ley española añade es certeza sobre el régimen sancionador nacional, la arquitectura de supervisión y las especificidades propias del ordenamiento jurídico español.

Para empresas como agencias de marketing, consultoras digitales o cualquier empresa que use IA en procesos que afecten a personas, las prioridades estratégicas son:

- Actuar ahora, no esperar a 2027. Las obligaciones del Artículo 4 (formación) y las prohibiciones ya son exigibles. La ventana educativa de la AESIA es temporal.
- Empezar por el inventario. Sin saber qué sistemas de IA usas y cómo los clasificas, ninguna otra acción es posible.
- Tratar el compliance de IA como parte del compliance de datos, no como un proyecto separado. RGPD y AI Act se solapan en el 80% de los casos de uso.
- Documentar todo. En caso de investigación, la diferencia entre una multa máxima y una sanción reducida o archivada será la evidencia de diligencia.
- No asumir que usar herramientas de terceros (ChatGPT, Gemini, etc.) exime de responsabilidad. Como deployer, eres responsable del uso que haces de esas herramientas en tu contexto de negocio.
- Vigilar la tramitación parlamentaria. El texto puede sufrir modificaciones antes de su aprobación definitiva. Las enmiendas en el Congreso pueden alterar el régimen sancionador, las definiciones o las exenciones.

Reflexión final

España tiene una oportunidad real de convertirse en un referente europeo en IA responsable. La AESIA es pionera, el sandbox está activo y la ley está en marcha. Para las empresas que se adelanten, el cumplimiento temprano no es solo gestión de riesgo: es una ventaja competitiva en un mercado donde clientes, inversores y licitadores públicos empezarán a exigir evidencias de gobernanza de IA como condición de negocio.