1

Empresas que empiezan a conocer el Reglamento

Guía 1. Introducción al Reglamento IA

Reglamento Europeo de Inteligencia Artificial

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

Esta guía ha sido desarrollada en el marco del desarrollo del piloto español de sandbox regulatorio de IA, en colaboración entre los participantes, asistencias técnicas, potenciales autoridades nacionales competentes y el grupo asesor de expertos del sandbox.

La guía tiene como objetivo servir de apoyo introductorio a la normativa europea de Inteligencia Artificial y sus obligaciones aplicables. Si bien **no tiene carácter vinculante ni sustituye ni desarrolla la normativa aplicable, proporciona recomendaciones prácticas** alineadas con los requisitos regulatorios a la espera de que se aprueben las normas armonizadas de aplicación para todos los estados miembros.

El presente documento está sujeto a un **proceso permanente de evaluación y revisión**, con actualizaciones periódicas conforme al desarrollo de los estándares y las distintas directrices publicadas desde la Comisión Europea, y será actualizada una vez se apruebe el Ómnibus digital que modifica el Reglamento de Inteligencia Artificial.

Fecha de versión: 10 de diciembre de 2025

Índice detallado

1. Preámbulo

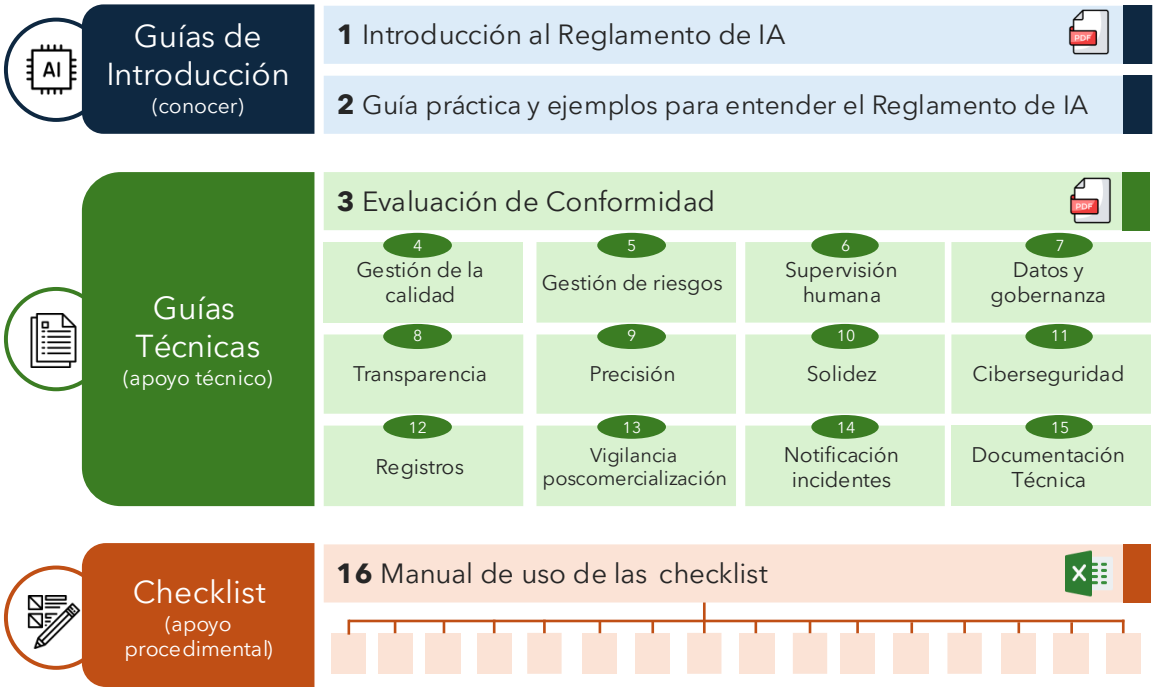
1.1 Objetivo del documento

El propósito de la presente guía introductoria es ofrecer una **comprensión general del Reglamento Europeo de Inteligencia Artificial (Reglamento de IA),** facilitando al lector que se inicia en la materia una visión clara sobre su alcance normativo, su ámbito de aplicación y las principales obligaciones que de él se derivan. Su objetivo es servir **como punto de partida para familiarizarse con los elementos esenciales del Reglamento**, abordando de manera breve y estructurada los conceptos clave que sustentan su contenido. En este sentido, se presentará el contexto normativo en el que se inscribe el Reglamento de IA, su finalidad dentro del marco jurídico europeo y las implicaciones que tiene para los distintos actores involucrados en el desarrollo, implementación y uso de sistemas de inteligencia artificial (IA).

A lo largo de las siguientes secciones, se identifican el **ámbito de aplicación del Reglamento**, la **gobernanza de supervisión**, los **roles y responsabilidades** en la cadena de valor de desarrollo de sistemas IA definidos por el Reglamento, así como la correspondencia entre los **tipos de sistemas de IA y los niveles de exigencia que les resultan aplicables**. De igual modo, se ofrece un **resumen de las obligaciones más relevantes según el nivel de riesgo del sistema**, acompañado de una breve descripción.

Para aquellas personas o entidades que deseen profundizar en aspectos específicos, como por ejemplo las obligaciones exigibles a sistemas de IA de alto riesgo, se ponen a disposición **guías técnicas especializadas** sobre cada requisito, complementadas con una **Guía práctica y ejemplos para entender el Reglamento de IA** que articula su relación conjunta, con el fin de favorecer una comprensión coherente y completa del marco regulatorio. Las guías, que se corresponden a artículos del Reglamento de IA, están desarrolladas de manera que se puede establecer una relación entre ellas, tal y como se ilustra en la siguiente imagen:

ILUSTRACIÓN 1: RELACIÓN DE GUÍAS DEL RIA



La presente guía toma como referencia el Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento Europeo de Inteligencia Artificial).

2. Introducción

2.1 Introducción al Reglamento Europeo de IA

La rápida **expansión de la inteligencia artificial (IA)** ha transformado la forma en que las organizaciones abordan la gestión de datos, la automatización de procesos y la toma de decisiones. Su capacidad para analizar grandes volúmenes de información, identificar patrones y generar predicciones precisas la convierte en una **herramienta esencial para la eficiencia y la innovación en múltiples sectores.** Sin embargo, junto a sus ventajas emergen también importantes desafíos éticos, sociales y jurídicos que requieren una atención especial.

Las peculiaridades que asemejan los sistemas de IA a los seres humanos –especialmente en lo relativo a la toma de decisiones autónomas– han suscitado **preocupación tanto por los posibles impactos sociales como por los riesgos inherentes a su uso**. Entre ellos destacan la delegación excesiva de decisiones críticas (por ejemplo, en el ámbito médico o jurídico) o la aparición de sesgos que pueden derivar en discriminaciones por razón de sexo, raza o edad. Por este motivo, se hace **necesario el establecimiento de requisitos de seguridad y calidad de los sistemas de IA**, **en función de su grado de riesgo,** de cara a promover un uso seguro de esta tecnología y se minimicen los posibles daños.

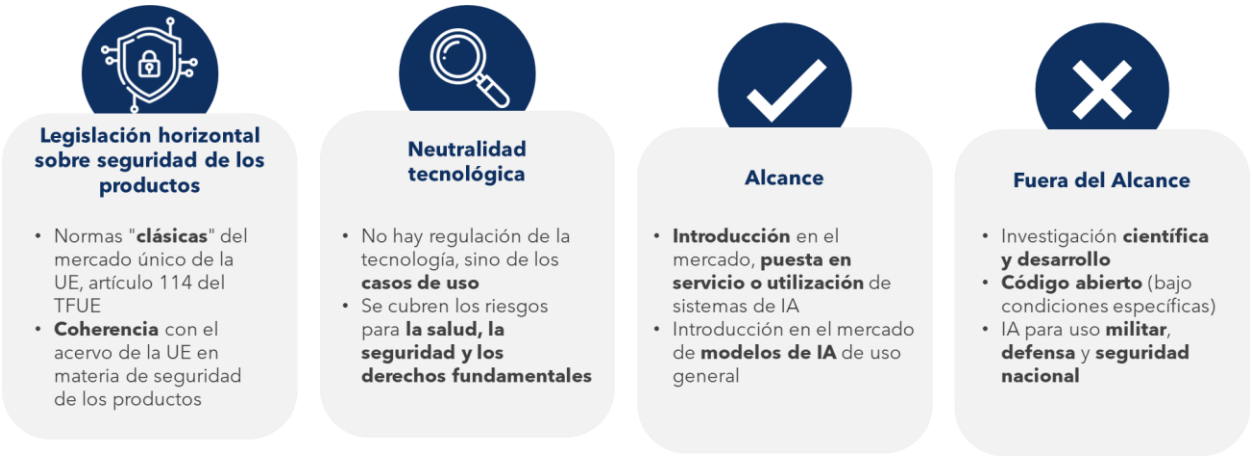
En esta línea, **organismos internacionales como la UNESCO, la OCDE y la Unión Europea coinciden en que el ser humano debe permanecer siempre en el centro del desarrollo tecnológico**, manteniendo la IA como herramienta de apoyo y complemento. Sobre este principio se asientan los principios para definir un marco seguro en el uso de la inteligencia artificial:

- **Evitar sesgos y la no-discriminación.** Evitar que los algoritmos tengan problemas de discriminación y buscar la manera de que los resultados obtenidos sean explicables.
- **Ciberseguridad, solidez y precisión.** Asegurar que los sistemas de IA sean robustos frente a ataques cibernéticos, manipulaciones o alteraciones no autorizadas, y que mantengan un comportamiento estable, predecible y exacto incluso en condiciones adversas.
- **Sistema de gestión de calidad y sistema de gestión de riesgos.** Implementar un marco integrado que asegure la documentación, trazabilidad, pruebas y mantenimiento continuo de los sistemas y que permita identificar, evaluar y mitigar los riesgos para la salud, seguridad y los derechos fundamentales, y aplique controles preventivos y correctivos durante todo el ciclo de vida del sistema.

Con el objetivo de garantizar la seguridad y fiabilidad de los sistemas, a la vez que promover un uso ético y responsable de la IA, la Unión Europea ha desarrollado el **Reglamento Europeo de Inteligencia Artificial**, cuyo propósito general es asegurar el adecuado funcionamiento del mercado interior mediante el establecimiento de requisitos que deben implementarse durante el desarrollo y uso de sistemas de IA. Es decir, este Reglamento busca crear un **ecosistema de confianza** sustentado en un marco jurídico que fomente la innovación responsable y la protección de los derechos fundamentales.

El Reglamento de Inteligencia Artificial define el siguiente **contenido o alcance regulatorio**:

ILUSTRACIÓN 2: CONTEXTUALIZACIÓN REGLAMENTO IA



Por otro lado, están los objetivos del Reglamento, que expresan las **metas o finalidades** que la Unión Europea busca alcanzar mediante esta norma. Entre ellos se destacan:

- **Garantizar que los sistemas de IA** comercializados o puestos en funcionamiento en la Unión Europea **sean seguros** y respeten la legislación vigente y los valores de la UE.
- Proporcionar seguridad jurídica para **favorecer la inversión y la innovación**.
- Mejorar la gobernanza y la aplicación efectiva de la normativa sobre **derechos fundamentales y seguridad en el uso de la IA**.
- **Definir un mercado único para la IA**, que permita un uso confiable y seguro de la inteligencia artificial, evitando la fragmentación regulatoria.

De este modo, ética y regulación se presentan como pilares complementarios: la primera orienta el desarrollo responsable de la tecnología, y la segunda establece el marco normativo necesario para garantizar su uso seguro y confiable en beneficio de toda la sociedad.

El artículo 2 del Reglamento define con precisión sus **límites de aplicación**, estableciendo qué sistemas de inteligencia artificial quedan fuera de su alcance. Estas exclusiones buscan equilibrar la regulación de los sistemas de IA con la necesidad de proteger actividades sensibles y fomentar la innovación tecnológica. Entre los principales ámbitos excluidos se incluyen:

1. **Investigación y desarrollo (I+D).** El Reglamento no se aplica a los sistemas o modelos de IA que se desarrollen específicamente con fines únicos de investigación científica y desarrollo. Tampoco será aplicable a ninguna actividad de investigación, prueba o desarrollo relativo a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Las pruebas en condiciones reales no estarán cubiertas por esta exclusión.

2. **Militar, defensa o seguridad nacional.** Los sistemas de IA utilizados exclusivamente con fines militares, de defensa o de seguridad nacional quedan fuera del ámbito del Reglamento, independientemente de la entidad que los utilice o del lugar donde se

comercialicen o pongan en servicio. Esta exclusión también se extiende a los sistemas de IA que no se comercialicen en la Unión, pero cuyo producto se utilice dentro de ella únicamente con dichos fines.

3. **Software *open -source*.** Los sistemas de IA liberados bajo licencias libres o de código abierto no están sujetos al RIA, salvo que se comercialicen o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas con obligaciones de transparencia. No podrán utilizarse para los fines que el Reglamento de IA prohíbe.

4. **Uso por parte de personas físicas en ámbito no profesional.** El Reglamento no se aplica en el uso de IA personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.

2.2 Gobernanza de supervisión de mercado

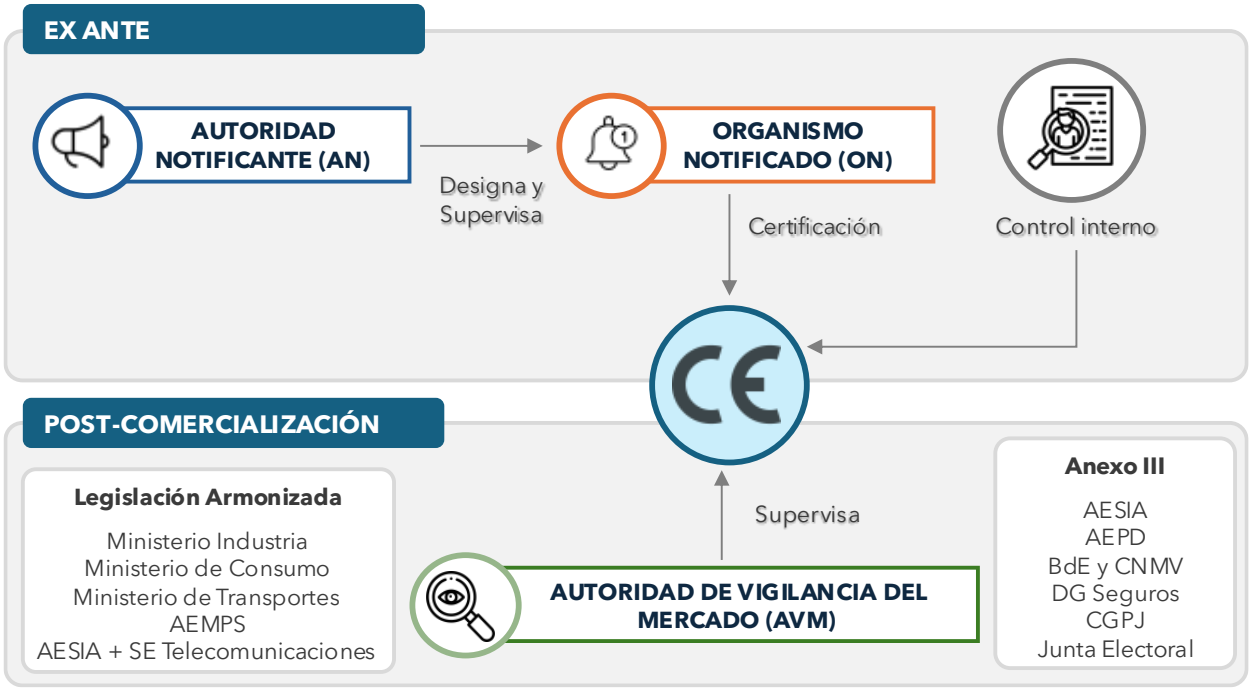
La gobernanza en el marco del Reglamento Europeo de IA se estructura sobre un modelo multinivel que combina supervisión europea y nacional, con el objetivo de garantizar la correcta aplicación, control y coherencia del Reglamento en todos los Estados miembros. En concreto, cada Estado miembro debe designar una serie de Autoridades Nacionales Competentes: las Autoridades de Vigilancia del Mercado (AVM) y las Autoridades Notificantes (AN).

Las Autoridades de Vigilancia del Mercado (AVM) desempeñan una función operativa de control, inspección y supervisión del cumplimiento. Son las encargadas de verificar que los sistemas de IA puestos en el mercado o en servicio cumplen los requisitos establecidos, pudiendo imponer medidas correctivas o sancionadoras en caso de incumplimiento.

Las Autoridades Notificantes (AN) serán las responsables de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión. Estas autoridades, sólo podrán notificar aquellos organismos que hayan cumplido los requisitos específicos que establece el propio Reglamento.

Además, aunque no son Autoridades Nacionales Competentes, también tienen un papel relevante los llamados **Organismos Notificados (ON).** Son aquellos organismos de evaluación de conformidad independientes de los sistemas de IA de alto riesgo que han sido debidamente notificados por la AN. Su papel es garantizar una verificación técnica y objetiva del cumplimiento de los requisitos aplicables antes de la comercialización o puesta en servicio del sistema conforme al Anexo VII en aquellos casos en los que es necesaria la participación de un tercero.

Ilustración 3: Gobernanza del reglamento de IA



2.3 Niveles de riesgo del Reglamento Europeo de IA

El Reglamento no regula la tecnología en sí misma -lo cual permitirá que continúe vigente ante la expansión de la frontera técnica- sino el uso que de ella se haga. Es **una regulación basada en el riesgo de cada sistema de IA,** de modo que, a mayor riesgo, se ejerza mayor control. Así, establece la siguiente clasificación:

Ilustración 4: Clasificación de sistemas de IA según el riesgo

A) Sistemas prohibidos: los usos de IA que se encuentren en este nivel de la jerarquía están prohibidos debido al alto riego que entrañan: sistemas IA que suponen una amenaza para la seguridad, la vida o los derechos fundamentales. En este nivel se encuentran, por ejemplo, los sistemas con alguna de las siguientes funciones:

- Manipulación subliminal del comportamiento de una persona de manera que pueda causarle daños físicos o psicológicos a él o a otros.
- Explotación de vulnerabilidades de grupos sociales para manipular su comportamiento de forma que pueda causarles daño a ellos o a otros.
- Evaluación o clasificación de personas o grupos por su comportamiento social que pueda perjudicarlos desproporcionadamente en el ámbito del comportamiento observado, o perjudicarlos en ámbitos distintos a donde se observó.
- Identificación biométrica en tiempo real en espacios de acceso público para autoridades policiales, salvo casos tasados y mediando autorización.

La Comisión Europea ha preparado unas directrices con el fin de aclarar la interpretación de ciertos casos concretos (*Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 20241689 (AI Act)*)[1].

B) Sistemas de Alto Riesgo: el segundo nivel se reserva a los sistemas de alto riesgo, pero cuyo uso está permitido, a los que el Reglamento dedica la mayoría de los requisitos y obligaciones que deben cumplir los distintos roles que participan en la cadena de valor de la puesta en uso de un sistema IA (operadores). Se dividen en dos tipos de sistemas:

B1) Productos o componentes de seguridad de alto riesgo contemplados en legislación de armonización:

- Sistemas de IA que sea un componente de seguridad de alguno de los productos contemplados en la legislación de armonización de la Unión recogidos en el Anexo I del Reglamento o,
- Que el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a dicha legislación de armonización.

En ambos casos, la **evaluación de conformidad del sistema de IA** deberá realizarse **como parte de la evaluación de conformidad del producto** conforme a la legislación de armonización aplicable.

La legislación de armonización de cada uno de los productos o componentes de seguridad de los productos se menciona en el **Anexo I Sección A** del Reglamento Europeo de la IA. **Dichos productos son**: máquinas, juguetes, ascensores, equipo y sistemas de protección para uso en atmósferas potencialmente explosivas, equipos radioeléctricos, equipos a presión, equipos de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios, productos sanitarios para diagnóstico in vitro, automoción y aviación.

[1] Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 20241689 (AI Act)

En el contexto de la evaluación de la conformidad, cuando los actos legislativos del anexo 1, sección A permitan al fabricante prescindir de la evaluación de un tercero, a condición de que el fabricante haya aplicado todas las normas armonizadas que contemplan todos los requisitos pertinentes, **dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado las normas armonizadas, o en su caso las especificaciones comunes** a las que se refiere el Reglamento.

B2) Finalidades de alto riesgo:

Sistemas de IA que se utilizan con finalidades que se consideran que presentan un alto riesgo para la salud, la seguridad y/o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca.

Estas finalidades se mencionan en el **Anexo III** del Reglamento Europeo de la IA. En concreto, **estas finalidades son:** biometría, infraestructuras críticas, educación y formación profesional, empleo, gestión de los trabajadores y acceso al autoempleo, acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales, garantía del cumplimiento del Derecho, migración, asilo y gestión del control fronterizo y administración de justicia y procesos democráticos.

En el contexto de la evaluación de la conformidad, **los sistemas de alto riesgo enumerados en el Anexo III punto 1**, el proveedor haya aplicado las normas armonizadas o especificaciones comunes **podrá optar por un procedimiento de evaluación de la conformidad con la participación de un organismo notificado o bien fundamentado en el control interno** (autoevaluación), mientras que **los sistemas de los puntos 2 a 8 se atendrán a este último**.

C) Sistemas con obligaciones de transparencia: La regulación establece la obligación de transparencia hacia los usuarios para este tipo de productos. Entre otras cosas, están obligados a dejar claro que su salida es producto de un sistema de inteligencia artificial, no de un humano. En este nivel se encuentran los *chatbots* y los sistemas de creación de *deep fakes*, entre otros.

En el caso de estos sistemas se establece la **obligación de informar a los usuarios** de dichos sistemas de que están llevando a cabo una interacción con un sistema de IA, y no un ser humano, además del **etiquetado de todo contenido (vídeo, audio, texto, etc.) sintético**, generado a través de IA.

D) Resto de sistemas de IA: para el resto de los sistemas de IA se contemplan únicamente obligaciones básicas, como la formación a los usuarios de los sistemas en materia de IA (alfabetización). Entre ellas se encuentra la aplicación de la IA a los videojuegos o los filtros de spam para el correo electrónico.

E) Sistemas no considerados de IA: determinados algoritmos más clásicos, como los basados en reglas o heurísticas, no son considerados sistemas de IA en el marco del Reglamento, y por tanto no les aplica.

El Reglamento, además, regula los **modelos de IA de uso general (GPAI)**, modelos de IA típicamente entrenados con un gran volumen de datos y que es capaz de realizar de manera competente una gran variedad de tareas distintas como la respuesta a preguntas, la

traducción, la generación de todo tipo de contenido, etc. Estos modelos **pueden adaptarse a una gran variedad de tareas mediante configuración o entrenamiento posterior**. Según su integración en un sistema de IA con un propósito concreto, el sistema podrá considerarse de alto riesgo o incluso de uso prohibido.

En función de su tamaño y de los riesgos derivados de su uso, se habla de modelos de IA de uso general y de modelos de IA de uso general de riesgo sistémico. Se establecen obligaciones diferenciadas para estos modelos que van desde:

- Obligaciones de transparencia.
- Elaboración de documentación técnica.
- Directrices sobre el cumplimiento de la normativa sobre derechos de autor.
- Evaluación del modelo, mitigación de riesgos, registro y comunicación de incidentes graves.

El Reglamento de IA es más flexible en cuanto a las obligaciones normativas respecto de los modelos de IA de uso general que sean de código abierto o licencia gratuita.

Para facilitar el cumplimiento de los requisitos impuestos a los proveedores de modelos de propósito general, la Comisión ha publicado un código de práctica de IA de propósito general[2] compuesto por tres capítulos: transparencia, propiedad intelectual y seguridad. Este código se acompaña de unas directrices[3] para los proveedores de este tipo de modelos. Mediante estas herramientas la Oficina de IA busca proporcionar un marco de certidumbre que garantice el cumplimiento normativo de los GPAI.

2.4 Operadores en el Marco del Reglamento Europeo de IA

El **Reglamento Europeo de la IA** menciona todos los potenciales **roles que participan en la cadena de valor de los sistemas de IA (operadores)**. El objetivo es establecer las responsabilidades que cada uno de estos roles debe asumir durante el ciclo de vida de los sistemas de IA.

2.4.1 Definiciones de los operadores según el Reglamento de IA

Proveedor
Persona física o jurídica, autoridad pública, agencia u otro organismo que **desarrolle o haga desarrollar un sistema** de IA o un modelo de IA de uso general **y lo introduzca en el mercado o lo ponga en servicio bajo su propio nombre o marca comercial**, ya sea a título oneroso o gratuito.
Responsable del despliegue

[2] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
[3] https://ec.europa.eu/newsroom/dae/redirection/document/118340

Cualquier persona física o jurídica, autoridad pública, organismo o cualquier otra entidad que **utilice un sistema de IA bajo su autoridad**, salvo cuando dicho uso se enmarque en una actividad personal de carácter no profesional.
Representante autorizado
Persona física o jurídica ubicada o establecida en la Unión que haya **recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones** y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor.
Importador
Toda persona física o jurídica físicamente presente o establecida en la Unión que **introduzca en el mercado un sistema de IA que lleve el nombre o la marca comercial de un sistema IA procedente de una persona física o jurídica establecida fuera de la Unión**. Introducen en el mercado por primera vez el sistema de IA para comercializar en el nombre o marca de una persona física o jurídica establecida fuera de la Unión, ya se produzca e suministro de manera remunerada o gratuita.
Distribuidor
Toda persona física o jurídica que forme parte de la cadena de suministro, distinta de proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión. Comercializan los sistemas, esto es, **suministran un sistema de IA para su distribución o utilización en el mercado de la Unión** en el transcurso de una actividad comercial, ya se produzca el suministro de manera remunerada o gratuita.

2.4.2 ¿Cuándo un responsable del despliegue u otras personas pasan a tener que cumplir las obligaciones de proveedor?

El Reglamento contempla diversas circunstancias en las que diferentes sujetos distintos al proveedor asumen las obligaciones que a priori están asignadas a este último.

En concreto, **cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor** de un nuevo sistema de IA de alto riesgo a efectos del Reglamento **si se producen alguna de las siguientes circunstancias:**

- **Ponen su nombre o marca en un sistema de IA de alto riesgo** que **ya** se ha **introducido** en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulan que las obligaciones se asignen de otra manera.

- **Realizan una modificación sustancial** de un sistema de IA de alto riesgo que ya se ha introducido en el mercado o puesto en servicio.

- **Modifican la finalidad prevista de un sistema** de IA que no es de alto riesgo y que ya está introducido en el mercado o puesto en servicio, **de manera que** el sistema modificado se convierte en un sistema de IA de alto riesgo.

Debe llamarse la atención de la importancia de estas situaciones de modificación de las finalidades previstas o alteración de la finalidad prevista.

Ello tendrá, obviamente, claras implicaciones en las responsabilidades de unos y otros sujetos. Cuando se den estas circunstancias, el proveedor que inicialmente introdujo en el mercado o puso en servicio el sistema de IA de alto riesgo dejará de ser considerado proveedor a efectos del Reglamento, si dichos cambios los ha realizado otro operador.

2.4.3 Particulares de los operadores del sector público

Como norma general, **el Reglamento se aplica por igual a las organizaciones privadas, a las administraciones públicas y a las entidades del sector público**. Ahora bien, se establece la obligación adicional para sistema de alto riesgo, que consiste en el desarrollo de una **evaluación de impacto relativa a los derechos fundamentales**.

Con el objetivo de garantizar eficazmente la protección de los derechos fundamentales por medio de la determinación de los riesgos específicos para los derechos de las personas y colectivos que se vean afectados.

EIDF o FRIAs **(Evaluación de Impacto relativa a los derechos fundamentales)**
Obligatoria **antes del despliegue** de un sistema de alto riesgo* Realizada por **responsables de despliegue.**
Contenido • Descripción procesos de uso del sistema. • Período de tiempo y frecuencia de uso. • Categoría personas físicas y colectivos afectados • Riesgos de perjuicio específicos • Descripción medidas de supervisión humana • Medidas en caso de que el riesgo se materialice (Mecanismos de reclamación)
Sistema utilizado en **casos similares**, responsable de despliegue **basarse en EIDF realizadas previamente o existentes.** Parte del **contenido ya incluido en EIPD** (Evaluación de Impacto de Protección de Datos), **EIDF la complementará.**
Notificación a AESIA (Pendiente de publicación modelo cuestionario por la AI Office)

*Excepción: Infraestructuras Críticas

2.4.4 Pequeñas y Medianas empresas (PYME), incluidas las empresas emergentes o start-ups[4]

El Reglamento presta una atención especial a las pequeñas y medianas empresas, incluidas las empresas emergentes proveedoras y responsable del despliegue de sistemas de IA.

Así, se prevén diversas obligaciones que han de adoptar tanto la Comisión Europea como los Estados Miembros en favor de estas organizaciones cuando asuman el papel de responsables del despliegue o proveedores. Facilitando el cumplimiento del Reglamento adaptando las obligaciones en función de su capacidad y tamaño, garantizando una correcta seguridad final del sistema de IA.

Una de las particularidades de las pymes se deriva del régimen sancionador. Como regla general, cuando una organización es sancionada de acuerdo con el Reglamento, la multa impuesta debe ser la mayor de las cuantías correspondientes al importe total asignado a esa infracción o al porcentaje específico asignado a esa infracción respecto del volumen de negocios de esa organización. Sin embargo, para el supuesto de las pymes, la multa impuesta podrá ser la menor de las cuantías de los importes previamente indicados.

En la imagen inferior se identifican algunas de las particularidades previstas para las pequeñas y medianas empresas en el Reglamento de IA.

Ilustración 5: Particularidades pymes, empresas emergentes y start-ups

Particularidades de PYMEs, empresas emergentes y start-ups
• Sanciones en la cuantía inferior entre importe o porcentaje (ver texto anterior). • Acceso prioritario a sandboxes. • Canales específicos de asesoramiento y consultas. • Modelos normalizados para el cumplimiento del Reglamento. • Reducción de carga documental técnica y de tasas durante el proceso de evaluación de conformidad. • Sistemas de Gestión de Calidad adaptados proporcionalmente al tamaño de la empresa.

2.5 Espacios Controlados de Pruebas para la IA

El artículo 57 del Reglamento desarrolla la regulación para el establecimiento de **espacios controlados de pruebas (sandbox) para la inteligencia artificial, con el ánimo de apoyar la innovación en IA**. Se trata de entornos controlados de pruebas, supervisados por las autoridades competentes que fomente la innovación y facilite el desarrollo, el entrenamiento,

[4] La mayor parte de las particularidades aplicadas a PYME en el reglamento se extienden a pequeñas empresas de mediana capitalización (SMC) en el texto del Digital omnibus elevado al Parlamento Europeo. Se entiende por éstas aquellas que no siendo PYME tiene menos de 750 empleados y cuyo volumen de negocios anual no excede de 150 millones EUR o cuyo balance general anual no excede de 129 millones EUR.

la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio.

A petición del proveedor, la autoridad competente del sandbox aportará un informe de salida que detallarán las actividades llevadas a cabo y los resultados. Esta documentación podrá ser utilizada por los proveedores para demostrar su cumplimiento con el Reglamento mediante el proceso de evaluación de conformidad o las actividades de vigilancia de mercado pertinentes. **Las AVM y los ON tendrán en cuenta positivamente los informes y pruebas, con vistas a acelerar los procedimientos** en una medida razonable, sin que ello implique una exención de las obligaciones ni sustituya los procedimientos formales de evaluación de la conformidad.

3. Principales Obligaciones

En la presente sección se detallan ciertas de las obligaciones más importantes del Reglamento de IA para los distintos operadores.

3.1 Obligaciones de alfabetización de IA

Se contemplan una serie de obligaciones generales aplicables a todas las entidades que actúen como proveedoras o responsables de despliegue de sistemas de IA en cuanto a alfabetización en la organización.

Conforme al artículo 4, toda entidad que introduzca en el mercado o utilice sistemas de IA debe promover la alfabetización en materia de IA. Para ello, se debe tratar de que **el personal que se encargue del funcionamiento de los sistemas tenga un conocimiento suficiente en materia de Inteligencia Artificial**.[5]

3.2 Obligaciones de transparencia

El artículo 50 establece obligaciones de transparencia, que **exigen a los proveedores y responsables del despliegue informar de manera clara y comprensible** cuando las personas interactúan con un sistema de IA, cuando se generan contenidos sintéticos (por ejemplo, texto, imágenes o vídeo) o cuando se emplean técnicas de reconocimiento emocional o biométrico. En dichos casos será necesario indicar el uso de un sistema de IA:

- Cuando un sistema interactúe directamente con personas físicas deberá informarse de que se está interactuando con un sistema de IA.
- Cuando un sistema de IA de uso general genere contenido sintético, se deberá garantizar que el contenido esté marcado en un formato legible por máquina y que sea posible detectar que ha sido generado o manipulado de manera artificial.
- Los responsables del despliegue de un sistema de IA que genere *deepfakes*, hará público que el contenido ha sido generado o manipulado de manera artificial.
- Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial.

3.3 Obligaciones de los sistemas de alto riesgo

A continuación, se describen de forma concisa las obligaciones que deben cumplir los **proveedores** de sistemas de alto riesgo de acuerdo con el Reglamento de IA:

[5] De acuerdo con el texto del Digitial omnibus elevado al Parlamento Europeo la obligación de alfabetización se sustituye por fomentar que todo usuario del sistema tenga conocimientos y formación adecuada en IA.

Sistema de gestión de riesgos (artículo 9)

Un sistema de gestión de riesgos tiene por objetivo la identificación y análisis de riesgos y la implementación de medidas que mitiguen su impacto. En el contexto del Reglamento Europeo de la IA, el sistema de gestión de riesgos deberá prestar especial atención a la **identificación, análisis, evaluación y mitigación** de los **riesgos que afecten a la salud, la seguridad y los derechos fundamentales de las personas,** tanto en el uso previsto como en usos razonablemente previsibles. El Reglamento también incluye mecanismos de vigilancia, pruebas y actualizaciones sistemáticas, con énfasis en la mitigación técnica, el diseño adecuado, y la capacitación de los responsables del despliegue. El proceso de gestión de riesgos debe abordarse en todas las etapas del ciclo de vida del sistema de IA, desde el diseño y desarrollo hasta su comercialización y post comercialización.

Para saber más información, consulta la Guía de gestión de riesgos.

Datos y gobernanza de datos (artículo 10)

En el contexto de la IA, la **gobernanza de los datos es el conjunto de elementos** (políticas, procedimientos, procesos, normas, etc.) **que se implementan para garantizar que los datos utilizados en el entrenamiento, validación y prueba de los sistemas de IA son adecuados**, pertinentes, suficientemente representativos y cumplen los requisitos de calidad y completitud establecidos.
El Reglamento Europeo de la IA establece una serie de requisitos que deberá cumplir principalmente el proveedor de un sistema de IA de alto riesgo, entre los que se **exponen medidas organizativas y técnicas** que servirán a proveedores y responsables del despliegue. Estas medidas aplican en **cada una de las fases del modelo de gestión de datos** propuesto **para poder implantar un adecuado gobierno del dato**: requisitos de información, recopilación de datos, preparación, disposición de datos, eliminación de los mismos y seguimiento y mejora continua.

Para saber más información, consulta la Guía de datos y gobernanza del dato.

Documentación técnica (artículo 11)

Para **permitir la trazabilidad de los sistemas de IA de alto riesgo**, **verificar** si cumplen los **requisitos** previstos en el Reglamento, así como **vigilar su funcionamiento y llevar a cabo la vigilancia poscomercialización**, resulta esencial disponer de **documentación técnica** comprensible sobre el modo en que se han desarrollado y sobre su funcionamiento durante toda su vida útil. Esta documentación técnica tiene un papel muy relevante dentro del marco de evaluación de la conformidad.
A la hora de cumplir con esta obligación, es importante definir **cómo reflejar y estructurar esa documentación, y sobre cómo debe ser conservada**.
Esta obligación se complementa con la obligación de registro de todo sistema de alto riesgo contemplado en el Anexo III en una base de datos de la UE (artículo 49), salvo los relativos a infraestructuras críticas, que se registrarán en un registro nacional debido a su criticidad para la seguridad nacional.

Para saber más información, consulta la Guía de documentación técnica y conservación de la documentación.

Conservación de registros (artículo 12)

Un **registro es un archivo que almacena información sobre el comportamiento y desempeño del sistema** durante su entrenamiento o uso en producción. Por lo tanto, un **sistema de gestión de registros es un conjunto de procesos que se definen para recopilar, almacenar, analizar y gestionar los registros** generados por un sistema de IA. Los registros permiten a los desarrolladores y operadores del sistema entender cómo se comporta en diferentes situaciones y cómo se puede optimizar para mejorar su precisión y eficiencia. También puede ayudar a detectar errores o sesgos en el sistema.
Es necesario abordar el desarrollo de un adecuado sistema de gestión de registros, que no sólo permitirá cumplir con las exigencias del Reglamento, sino también **facilitará** otras tareas como la **transparencia y rendición de cuentas, y otras actividades de investigación y desarrollo basadas en pruebas.**

Para saber más información, consulta la Guía de registros y archivos de registro generados automáticamente.

Transparencia (artículo 13)

Transparencia es la cualidad de un **sistema de IA de poder ser interpretable y comprensible por todas las personas** que lo crean e interactúan con él en todo su ciclo de vida. El Reglamento Europeo de IA establece la obligación de procurar el diseño y desarrollo de sistemas que permitan a los responsables del despliegue **comprender y utilizar adecuadamente el sistema; proporcionar instrucciones de uso** que incluyan información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue; así como un **conjunto de información específica a tener en cuenta en el diseño y desarrollo del sistema**.

Para saber más información, consulta la Guía de transparencia y provisión de información a los usuarios.

Supervisión humana (artículo 14)

Las personas deben ser capaces de vigilar el funcionamiento de los sistemas de IA de alto riesgo. Para ello los sistemas deben proporcionar las **herramientas e interfaces necesarios para ejercer esa supervisión** e interactuar con ellos de manera segura. En otros términos, la supervisión humana ayuda a garantizar que un sistema de IA no socave la autonomía humana o provoque otros efectos adversos.
Las medidas están dirigidas, por tanto y específicamente, a un diseño y desarrollo específico de los sistemas de IA de alto riesgo, de forma que estos permitan realizar sobre ellos una vigilancia efectiva; el establecimiento de mecanismos para la prevención y minimización de los riesgos (sobre la salud, la seguridad, y los derechos fundamentales); la localización de la responsabilidad de proveedores y responsables del despliegue; la vigilancia informada y

consciente del sistema; y el aseguramiento de la vigilancia humana en aquellos sistemas que hacen uso de identificación biométrica.

Para saber más información, consulta la Guía de vigilancia humana.

Precisión (artículo 15)

Una manera clave de poder **mitigar al máximo los riesgos en el uso de la IA es la mejora de precisión de este sistema de IA**. A través de la precisión del sistema, obtenemos una medida cuantitativa de la relación entre la **finalidad prevista de este y su desempeño** desde el diseño hasta su funcionamiento tras la puesta en marcha del sistema de AI.
Esto se consigue a través de una serie de **medidas destinadas a que los sistemas de IA no degraden sus especificaciones de rendimiento y exactitud una vez puestos en marcha**. Para ello, deberán respetar niveles mínimos de precisión y/o métricas asociadas concretas a la tarea, preestablecidas, garantizando así que esta sea consistente durante todo el ciclo de vida.

Para saber más información, consulta la Guía de precisión.

Solidez (artículo 15)

Se entiende por **solidez técnica la resiliencia del sistema en relación con aquellos comportamientos perjudiciales**, o de otro modo indeseables, **que puedan derivarse de limitaciones en los sistemas o en el entorno en el que estos funcionan** (p. ej., errores, fallos, incoherencias o situaciones inesperadas). Por ello establece que el sistema de IA deberá considerar, en su **diseño, desarrollo y validación, las soluciones técnicas y organizativas para prevenir dichas situaciones**, previendo la posibilidad de que cuando dicha solidez técnica no opere dentro de parámetros seguros, el sistema pueda incluso interrumpir su funcionamiento.
Es **responsabilidad del proveedor** del sistema de inteligencia artificial de alto riesgo tomar las medidas adecuadas (tanto organizativas como técnicas) para garantizar que se cumple con los requerimientos de solidez del sistema. Igualmente, dentro de su ámbito de aplicación, el **responsable del despliegue del sistema también tiene responsabilidades** que se materializarán en medidas concretas (de nuevo organizativas y técnicas).

Para saber más información, consulta la Guía de solidez.

Ciberseguridad (artículo 15)

La ciberseguridad en sistemas de Inteligencia Artificial de alto riesgo es un aspecto clave de su diseño, ya que se trata de sistemas que se encuentran expuestos a amenazas específicas que requieren medidas de protección rigurosas y adaptadas a su contexto.
Las **medidas** de ciberseguridad incorporadas exigidas a un sistema de IA de alto riesgo tienen como objetivo **mitigar los riesgos que amenazan los derechos y libertades de las personas físicas y de la sociedad en general**, y se integran en marcos de gestión de la ciberseguridad más amplios. Estos se pueden ver seriamente amenazados por la existencia

de puertas traseras en los modelos, posibilidad ataques de exfiltración o vulnerabilidad a ataques adversarios.

Para saber más información, consulta la Guía de ciberseguridad.

Sistema de gestión de la calidad (artículo 17)

El Reglamento establece en su artículo 9 «*Sistema de gestión de la calidad*» requisitos en materia de calidad que deberán cumplir los proveedores de los sistemas IA de alto riesgo para **implementar un sistema de gestión de calidad documentado** que garantice el cumplimiento normativo. Este sistema debe incluir **estrategias de cumplimiento, gestión de riesgos, control de diseño y desarrollo, pruebas, vigilancia poscomercialización, notificación de incidentes y comunicación con autoridades y partes interesadas**. Su alcance debe ser proporcional al tamaño del proveedor y puede integrarse con sistemas existentes si cumplen normativas sectoriales de la UE.

Para saber más información, consulta la Guía de gestión de calidad.

Evaluación de la conformidad (artículo 43)

El Reglamento Europeo de IA establece que de acuerdo con el articulo 43 los sistemas de inteligencia artificial de alto riesgo deben someterse a un procedimiento de evaluación de conformidad previo a su comercialización o puesta en servicio. Este procedimiento distingue entre **control interno y evaluación por terceros**, en función de la naturaleza del sistema y de la aplicación de normas armonizadas.

Los sistemas de IA de alto riesgo que se encuentran sujetos al procedimiento de **evaluación basado en control interno definido en el Anexo VI** son los enumerados en los puntos 2 a 8 del Anexo III. Este procedimiento permite al proveedor llevar a cabo un control interno, verificando el cumplimiento de los requisitos esenciales establecidos en el Reglamento y la adecuación de su sistema de gestión de calidad conforme al artículo 17.

Los sistemas comprendidos en el punto 1 del Anexo III, en particular aquellos relativos a la identificación biométrica remota, podrán someterse al mismo procedimiento basado en control interno mencionado. No obstante, deberán someterse al procedimiento de evaluación de conformidad con intervención de un organismo notificado cuando no se hayan aplicado normas armonizadas o especificaciones comunes, según lo dispuesto en el **Anexo VII.**

Asimismo, en los casos en que el sistema de IA forme parte de un producto cubierto por legislación sectorial de armonización de la Unión (contemplado en el Anexo I, sección A), la evaluación de conformidad deberá integrarse dentro del procedimiento establecido para dicho producto, aplicándose las disposiciones previstas en el artículo 43(3) junto con los criterios técnicos definidos en los Anexos VI y VII.

Para saber más información sobre los procesos de evaluación de la conformidad véase el Anexo I de esta Guía y la Guía de evaluación de la conformidad.

Vigilancia de poscomercialización (artículo 72)
El Reglamento Europeo de IA introduce la necesidad de un establecer un sistema de vigilancia tras la puesta en marcha de los sistemas de inteligencia artificial de alto riesgo, en el marco de un plan de vigilancia de poscomercialización. Un plan de vigilancia poscomercialización es un **conjunto de actividades conducidas por los proveedores/usuarios**, para recolectar y evaluar la experiencia obtenida de sistemas de inteligencia artificial de alto riesgo que han sido **puestos en el mercado**, y así identificar la necesidad de tomar cualquier acción. Se trata de una herramienta importante para asegurar que los sistemas de IA siguen siendo seguros y funcionan correctamente. La **evaluación que se lleva a cabo con esta vigilancia poscomercialización puede contribuir, asimismo, a una continua mejora del sistema**. Para saber más información, consulta la Guía de vigilancia poscomercialización.
Notificación de incidentes graves (artículo 73)
El Reglamento define como obligación de los proveedores de HRAI la necesidad de **notificar cualquier incidente grave o defecto de un sistema de IA a las autoridades de vigilancia del mercado.** La notificación de incidentes graves conllevará el establecimiento de una coordinación con las autoridades europeas por parte de las autoridades nacionales competentes, con el objetivo de controlar y supervisar los incidentes más graves. Para saber más información, consulta la Guía de notificación de incidentes graves.

3.4 Fechas de activación de las obligaciones

<table>
<tr><th colspan="2">Tipo de sistema</th><th colspan="2">Fecha introducción mercado o puesta en servicio</th><th>Cumplimiento Obligaciones Reglamento de IA</th></tr>
<tr><td colspan="2">Prohibidos</td><td colspan="2">N/A</td><td>febrero 2025</td></tr>
<tr><td rowspan="4">Alto riesgo</td><td rowspan="2">Anexo I</td><td>Antes</td><td rowspan="4">2 agosto 2026</td><td>N/A, excepto sí cambios significativos (agosto 2027)
doce meses desde publicación comunicación (máximo agosto 2028)*</td></tr>
<tr><td>Después</td><td>agosto 2027
doce meses desde publicación comunicación (máximo agosto 2028)*</td></tr>
<tr><td rowspan="2">Anexo III</td><td>Antes</td><td>N/A, excepto sí cambios significativos (agosto 2026)
seis meses desde publicación comunicación (máximo diciembre 2027)*</td></tr>
<tr><td>Después</td><td>agosto 2026</td></tr>
</table>

				diciembre 2027*
	Utilizados por Autoridad Públicas	Antes		agosto 2030
Obligaciones de transparencia proveedor Art 50(2)		Antes	2 agosto 2026	agosto 2026 febrero 2027*
		Después		agosto 2026
Obligaciones de transparencia		Antes		agosto 2026
		Después		
GPAI		Antes	2 agosto 2025	agosto 2027
		Después		agosto 2026
		Modificación GPAI**		

* Versión actual del Digital Omnibus on AI

** Modificación > 1/3 entrenamiento sobre Modelo Base publicado antes de agosto 2025

4. ANEXO I. Evaluación de la conformidad de los sistemas de IA de alto riesgo y Autoridades de Vigilancia del Mercado

La presente tabla establece los distintos tipos de evaluación de la conformidad en función del sistema de IA de alto riesgo y la correspondiente Autoridad de Vigilancia del Mercado (AVM). Las AVM indicadas toman como referencia la designación establecida por el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial, y por lo tanto, su ratificación final dependerá de la aprobación de esta norma.

	Producto/sistema de IA	Autoridad de Vigilancia del Mercado	Tipo de evaluación
ANEXO I	Máquinas	SG Calidad y Seguridad industrial. Ministerio de Industria. (Según Anteproyecto de Ley)	Procedimiento según la legislación del producto
	Aparatos que queman combustible gaseoso		
	Equipos a presión		
	Instalaciones de transporte por cable		
	Protección individual		
	Ascensores		
	Protección para uso en atmósferas potencialmente explosivas		
	Equipos radioeléctricos	AESIA en colaboración con la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. Ministerio de Transformación digital.	
	Juguetes	DG Consumo. Ministerio de Consumo. (Según Anteproyecto de Ley)	
	Embarcaciones de recreo	DG Marina mercante. Ministerio de Transportes. (Según Anteproyecto de Ley	
	Productos sanitarios y Diagnóstico in vitro	Agencia Española del Medicamento. (Según Anteproyecto de Ley)	
ANEXO III	Infraestructuras críticas, Educación y formación, Empleo y Gestión de trabajadores, Acceso a servicios públicos, Priorización de servicios de emergencia.	AESIA (Según Anteproyecto de Ley)	Autoevaluación
	Identificación biométrica limitada		Autoevaluación u organismo notificado. Según apliquen o no

			normas armonizadas o especificaciones comunes.
	Scoring crediticio	BCE y CNMV (Según Anteproyecto de Ley	Autoevaluación
	Primas de seguros	DG de seguros y fondos de pensiones (Según Anteproyecto de Ley)	Autoevaluación
	Identificación biométrica para aplicación de la ley y para Gestión de fronteras	AEPD (Según Anteproyecto de Ley)	Autoevaluación u organismo notificado. Según apliquen o no normas armonizadas o especificaciones comunes.
	Aplicación de la ley y Gestión de Fronteras		Autoevaluación
	Identificación biométrica para Administración de Justicia	CGPJ (Aún por definir)	Autoevaluación u organismo notificado. Según apliquen o no normas armonizadas o especificaciones comunes.
	Administración de Justicia	CGPJ (Según Anteproyecto de Ley)	Autoevaluación
	Identificación biométrica para procesos democráticos/electorales	Junta electoral (Aún por definir)	Autoevaluación u organismo notificado. Según apliquen o no normas armonizadas o especificaciones comunes.
	Fines electorales/Democráticos /electorales	Junta electoral (Según Anteproyecto de Ley)	Autoevaluación

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de
Recuperación,
Transformación
y Resiliencia

España | digital 2026