

# Regulación legal de la inteligencia artificial

Introducción a la IA



# Regulación legal de la inteligencia artificial

A lo largo de estas páginas, aprenderemos acerca de la normativa aplicable en inteligencia artificial, dentro de la Unión Europea (UE), normativa que deberemos contemplar durante el desarrollo, la implementación y el uso de soluciones de inteligencia artificial (IA). También estudiaremos los bienes jurídicos, valores y libertades protegibles en este ámbito.

La inteligencia artificial (IA) puede aportar grandes beneficios para la sociedad, como mejorar la productividad, la sanidad, la educación, el transporte y otros ámbitos. Pero también puede suponer graves riesgos y perjudicar los intereses públicos y derechos fundamentales de las personas, causando daños físicos, psíquicos, sociales o económicos. Hay ejemplos de mal uso de la IA que han generado conflictos con los derechos de los ciudadanos, como el honor, la imagen, la intimidad, el empleo, la educación, la justicia o las libertades democráticas. Por eso, al desarrollar y utilizar sistemas de IA, se deben respetar valores como la igualdad, la libertad, la seguridad y la justicia, y evitar la exclusión social y la discriminación.

Así, nos adentraremos en el marco normativo establecido a nivel europeo para asegurar que los sistemas de IA que se usen en la UE sean fiables y seguros, y que cumplan con los derechos fundamentales, la democracia, el Estado de derecho y la protección del medio ambiente, que son los principios del Derecho de la UE. Entre otros, nos adentraremos en los requisitos que el Reglamento de Inteligencia Artificial de la UE aborda, en función de los distintos casos de uso previstos, obligaciones para los intervenientes en la cadena de valor, estudiaremos cuáles son los órganos de supervisión, así como las potenciales sanciones en caso de incumplimiento.

*Autor: Jesús Miguel Cativiela*

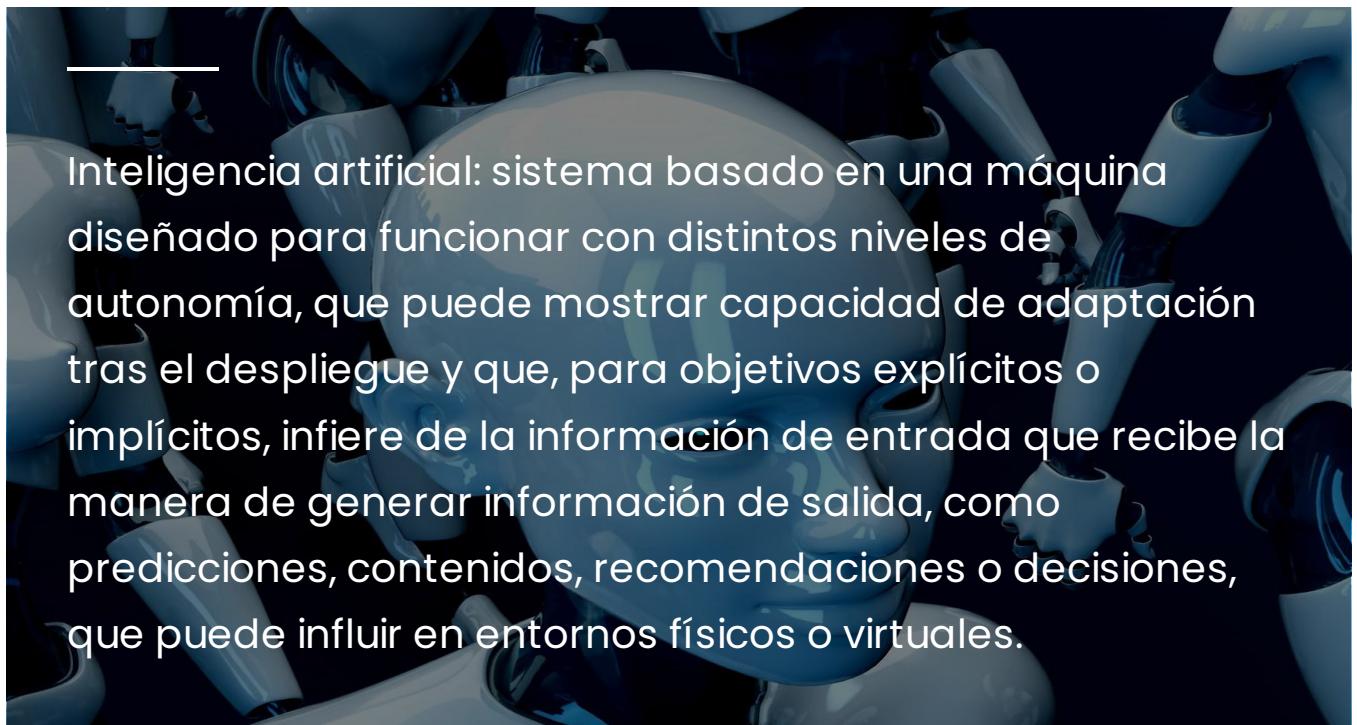
- Aproximación al Reglamento Europeo de IA
- Aplicabilidad, exenciones y principio de extraterritorialidad del Reglamento IA
- Enfoque desde la perspectiva de riesgo del Reglamento IA
- Modelos y sistemas de IA de uso general
- Espacios controlados de pruebas (sandbox)
- Gobernanza del Reglamento IA y sanciones
- Entrada en vigor y periodo de transición
- Conclusión

# Aproximación al Reglamento Europeo de IA



El legislador europeo ha establecido un marco de obligaciones uniformes que regula el desarrollo y uso de la IA en la UE, asegurando la libre circulación, innovación y despliegue en el mercado interior de los sistemas de IA, así como la garantía de una protección uniforme de los derechos fundamentales: el **Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial ([Reglamento IA](#))**.

El Reglamento IA es de aplicación directa en los Estados Miembros de la Unión Europea. Esto significa que no requiere ser aprobado por los parlamentos de los Estados Miembros de la UE para ser efectivo y, en consecuencia, puede ser invocado por los individuos ante los tribunales sin esperar a que haya una norma nacional que lo valide (efecto directo).



Inteligencia artificial: sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales.

Una cuestión clave es la definición de inteligencia artificial que recoge el Reglamento IA, lo que ha provocado mucha polémica y debate. La Comisión Europea proponía inicialmente una definición de IA demasiado amplia y vaga, que no se ajustaba a la rápida evolución de la que somos testigos en esta familia de tecnologías, ni a los estándares internacionales. Por eso, la definición que se usa en el Reglamento IA finalmente sigue el criterio internacional de la Organización para la Cooperación y el Desarrollo Económicos ([OCDE](#)), y dice lo siguiente...

Con esta definición de IA, se pretende influir de forma positiva en la **innovación tecnológica, la protección de los derechos individuales y la competitividad en el mercado global**, y distinguir la IA de los sistemas de software o los planteamientos de programación tradicionales y más sencillos que no tienen capacidad de inferencia (referida al proceso de obtención de información de salida). Aparte de esta definición de IA, los principales conceptos que debes conocer son los siguientes:

#### **Proveedor IA**

Una persona física, jurídica o autoridad que desarrolle un sistema o modelo de IA y que lo introduzca en el mercado o lo ponga en servicio con su propio nombre o marca comercial, previo pago o gratuitamente.

#### **Responsable del despliegue**

Una persona física, jurídica o autoridad que utilice un sistema de IA bajo su propia autoridad.

**Importador** —

Una persona física o jurídica, ubicada o establecida en la UE, que introduzca en el mercado un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida en un tercer país (fuera de la UE).

**Distribuidor** —

Una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la UE.

**Representantes autorizados** —

Una persona física o jurídica, ubicada o establecida en la UE, que haya recibido y aceptado el mandato por escrito de un proveedor IA para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el Reglamento IA en representación de dicho proveedor.

**Sistema de IA de uso general** —

Un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA.

# Aplicabilidad, exenciones y principio de extraterritorialidad del Reglamento IA



Bajo este epígrafe vamos a explicar algunos términos y principios que debes conocer y manejar para entender el Reglamento Europeo IA. ¡Toma nota!

## Aplicabilidad

El Reglamento IA tiene un enfoque transversal, siendo aplicable a una variedad de entidades y situaciones, tales como **proveedores IA** que pongan en servicio o comercialicen dentro de la UE, o cuya información de salida se utilice en la UE, independientemente de su origen, así como a los **responsables del despliegue** que explotan estos sistemas IA.

## Extraterritorialidad

El principio de extraterritorialidad implica que el Reglamento IA será aplicable también a los operadores económicos que desplieguen, introduzcan o pongan en servicio sistemas o modelos de IA en la UE, con independencia de que su sede esté ubicada fuera de la UE.

## Exenciones a la aplicación

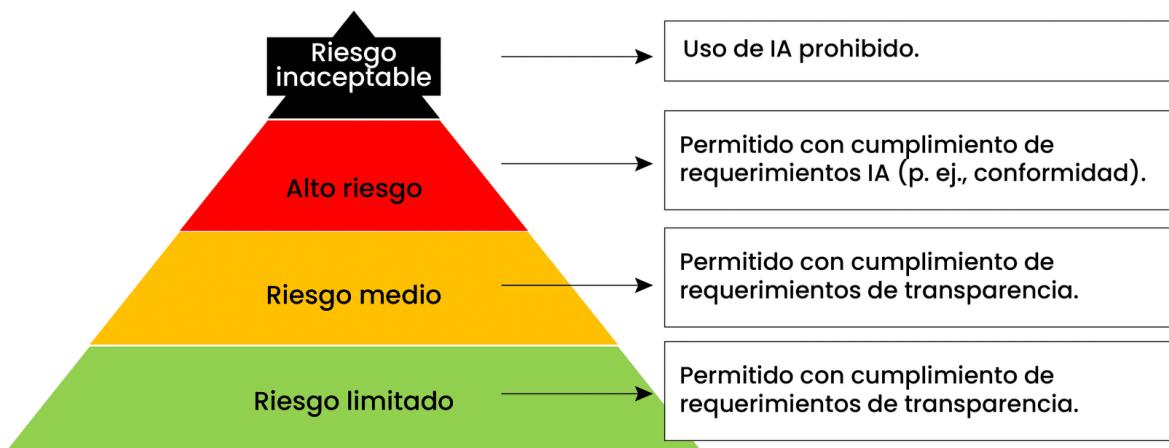
El artículo 2 del Reglamento IA establece **ciertos casos en los que el Reglamento IA no será aplicable**:

- **Militar y defensa:** sistemas IA utilizados para propósitos de defensa o militares.
- **I+D:** sistemas IA diseñados específicamente con la investigación y el desarrollo científicos como única finalidad.
- **Uso personal:** sistemas IA utilizados por personas en el ejercicio de una actividad puramente personal de carácter no profesional.
- **Código abierto:** sistemas de IA divulgados con arreglo a licencias libres y de código abierto, excepto si resultan ser sistemas de IA de alto riesgo, prohibidos o que interactúen directamente con personas físicas.
- **I+D de la IA:** la actividad de investigación, prueba o desarrollo relativa a sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio.

# Enfoque desde la perspectiva de riesgo del Reglamento IA



Para adaptarse a los avances tecnológicos, el Reglamento IA no regula tanto la tecnología en sí, sino el uso que se le puede dar. De este modo, fija **diferentes obligaciones según el nivel de riesgo de cada caso de uso**, clasificándolos en cuatro niveles: riesgo limitado, riesgo medio, alto riesgo y riesgo inaceptable.



## Riesgo inaceptable: usos prohibidos

Por implicar un riesgo inaceptable, el Reglamento IA incluye un listado de **usos que quedan totalmente prohibidos**. Estos son los siguientes:

1

### **Sistemas de IA que manipulan o engañan deliberadamente**

A las personas o se aprovechan de su vulnerabilidad por su potencial capacidad de generar daños físicos o psicológicos, mediante engaños, coacción o influencia en el comportamiento de forma perjudicial, o por su capacidad de aprovechar las debilidades de un individuo, exacerbando sus vulnerabilidades.

2

### **Sistemas de IA que explotan vulnerabilidades de una persona**

Como información que derive de la edad, la discapacidad o de una situación social o económica específica, con el objetivo o el efecto de alterar sustancialmente su comportamiento.

3

### **Sistemas de IA que evalúan o clasifican a personas en función de su comportamiento social**

O en función de características personales, inferidas o predichas, conllevando un trato perjudicial o desfavorable injustificado o desproporcionado.

4

**Sistemas de IA para realizar evaluaciones de riesgos de personas físicas**

Realizar evaluaciones de riesgos de personas físicas de cometer una infracción penal, basándose únicamente en la elaboración del perfil.

5

**Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial**

Basados en la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.

6

**Sistemas de IA para inferir las emociones de una persona física**

En los lugares de trabajo y en los centros educativos, excepto por motivos médicos o de seguridad.

7

**Sistemas de IA de categorización biométrica que clasifiquen individualmente a las personas físicas**

Sobre la base de sus datos biométricos para deducir o inferir raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida u orientación sexuales.

8

**Sistemas de IA de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley**, excepto para:

- búsqueda selectiva de personas desaparecidas, de víctimas de secuestro, trata o explotación sexual;
- prevención de una amenaza específica, importante e inminente para la vida o la seguridad física, o de un atentado terrorista;
- y localización o identificación de una persona sospechosa de haber cometido una infracción penal y castigada con al menos cuatro años de prisión.

## Alto riesgo

- **Determinación del alto riesgo**

El Reglamento IA establece que los sistemas de IA de Alto riesgo son aquellos que pueden **causar daños importantes a la salud, la seguridad o los derechos fundamentales, especialmente al tener un gran impacto en el resultado de las decisiones**. Para ello, el Reglamento IA lo aborda desde dos puntos de vista:

- Los sistemas de IA que se usan como parte de **productos sujetos a la legislación armonizada de la UE** y que necesitan una evaluación externa de su conformidad, por ejemplo, dispositivos médicos, mecanismos de seguridad de juguetes, equipos a presión, equipos radioeléctricos, vehículos de motor y remolques, etc.



Los **sistemas de IA que hacen perfiles de personas físicas** (que siempre se consideran de alto riesgo) y los que se listan en el **Anexo III del Reglamento de IA**, por ejemplo, los sistemas de IA biométricos o los empleados en infraestructuras críticas, educación y formación profesional, etc.



### **Excepciones a la cualificación de alto riesgo**

El Reglamento IA contempla casos en los que los sistemas de IA de alto riesgo no se clasifican como tales, si el sistema no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales, en particular al no influir sustancialmente en el resultado de la toma de decisiones, siempre y cuando se cumplan una o varias de las condiciones siguientes:



Que el sistema de IA tenga por objeto llevar a cabo una **tarea de procedimiento limitada**; por ejemplo: un sistema de IA que transforme datos no estructurados en datos estructurados.



Que el sistema de IA tenga por objeto **mejorar el resultado de una actividad humana previamente realizada**; por ejemplo: los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos ya redactados.



Que el sistema de IA tenga por objeto **detectar patrones de toma de decisiones** o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; por ejemplo: entre los sistemas de IA que pueden utilizarse para comprobar a posteriori si un profesor puede haberse desviado de su patrón de calificación determinado.

4

Que el sistema de IA tenga por objeto **llevar a cabo una tarea preparatoria** para una evaluación pertinente a efectos de los casos de uso enumerados en el Anexo III; por ejemplo: soluciones inteligentes para la gestión de archivos.

No obstante, tal y como se indicaba antes, **los sistemas de IA a que se refiere el Anexo III del Reglamento IA siempre se considerarán de Alto riesgo cuando se lleve a cabo la elaboración de perfiles de personas físicas** (es decir, utilizar datos personales para evaluar determinados aspectos personales de un individuo). **Además, cualquier IA de alto riesgo puede pasar a ser de riesgo inaceptable si da lugar a alguna de las circunstancias que se incluyen en el listado de prácticas prohibidas.**

●

#### **Obligaciones asociadas a los sistemas de alto riesgo**

En este epígrafe vamos a estudiar los **requisitos** que deben cumplir los sistemas IA de alto riesgo y las **obligaciones aplicables a los distintos operadores**.

### **Requisitos de los sistemas IA de alto riesgo**

Antes de su comercialización o puesta en servicio en la UE, los sistemas IA de alto riesgo deben cumplir con una serie de requisitos, ¡veamos cuáles son!

1

Sistema de gestión de riesgos: establecer y mantener un sistema que comprenda los riesgos conocidos y previsibles y medidas adecuadas y específicas que los mitiguen.

2

Datos y gobernanza: documentar que los datos utilizados para entrenamiento son pertinentes, representativos, sin errores y completos.

3

Documentación técnica: crear y mantener una documentación técnica en la que se detallen elementos tales como la finalidad prevista del sistema IA, su diseño o el proceso de desarrollo seguido.

4

Trazabilidad: deben tener capacidades de registro automático de eventos a lo largo de todo su ciclo de vida (registro de logs).

5

Transparencia: deben venir acompañados de unas instrucciones de uso con información concisa, completa, precisa y clara para los usuarios.

6

Sistema de supervisión humana: con el fin de que la persona supervisora entienda las capacidades y limitaciones del sistema, detectar anomalías o comportamientos inesperados, interpretar correctamente la información de salida, y decidir si desea utilizar el sistema o ignorar los resultados del mismo, así como su interrupción.

7

Precisión, solidez y ciberseguridad: los sistemas IA de alto riesgo deben alcanzar un nivel adecuado de precisión, solidez y ciberseguridad durante todo su ciclo de vida, que deben declararse en las instrucciones de uso (transparencia).

## Obligaciones para los proveedores de sistemas IA de alto riesgo

Además de lo anterior, los proveedores IA de sistemas de alto riesgo deben cumplir con una serie de obligaciones.

1

Cumplimiento requisitos de sistema de IA de alto riesgo: velar por el cumplimiento de los requisitos de los sistemas de alto riesgo que hemos visto antes.

2

Indicación de nombre, marca y dirección de contacto: indicar en el sistema IA (en su embalaje o en la documentación que lo acompañe, según proceda) el nombre, nombre comercial registrado y su dirección de contacto.

3

Sistema de gestión de calidad: debe recoger, entre otros contenidos, las técnicas utilizadas en el diseño, control y verificación; procedimientos de examen, prueba y validación, sistema de gestión de datos, de riesgos, de vigilancia poscomercialización, etc.

4

Documentación: conservar durante 10 años desde la entrada en el mercado o la puesta en servicio del sistema la documentación técnica, de calidad, de cambios aprobados y decisiones adoptadas por organismos notificados (si procede) y declaración UE de conformidad.

5

Archivos de registro generados por los sistemas IA: conservar los archivos de registro que los sistemas IA generen automáticamente, en la medida en que dichos archivos estén bajo su control.

6

Evaluación de conformidad (UE), declaración UE de conformidad y marcado CE: demostrar la conformidad del sistema IA, para lo que deben realizar un examen previo:

- con intervención de organismo notificado o de evaluación de conformidad (exigible para ciertos sistemas);
- o mediante un sistema basado en el control interno y la declaración de responsabilidad del proveedor.

Con posterioridad, el proveedor deberá redactar la declaración de conformidad correspondiente y obtener el marcado CE conforme al Reglamento 765/2008 para su comercialización.

7

Registro del sistema IA: registrar el sistema de alto riesgo en la base de datos de la UE o nacional (para IA relacionada con infraestructuras).

8

Adopción de medidas correctoras necesarias: si existen motivos para considerar que existe un incumplimiento con la regulación, deben corregirlo, retirarlo, desactivarlo o recuperarlo de inmediato e informar a otros operadores intervenientes en la cadena de valor del sistema IA (p. ej., a los responsables del despliegue, distribuidores, etc.), notificando de ello a las autoridades de vigilancia del mercado y al organismo notificado (los conceptos 'autoridad de vigilancia del mercado' y de 'organismo notificado' los estudiaremos más adelante en este fastbook).

9

Cooperación con autoridades y accesibilidad: deben suministrar a las autoridades competentes, bajo solicitud justificada, toda la información y documentación necesaria para demostrar la conformidad del sistema.

10

Accesibilidad: deben velar por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

## Obligaciones para los responsables del despliegue de sistemas IA de alto riesgo

Los responsables del despliegue de Sistemas IA de Alto riesgo deben cumplir una serie de deberes que, a continuación, vamos a presentar.

1

Uso conforme a instrucciones: usar sistemas IA de alto riesgo siguiendo las instrucciones de uso dadas por el proveedor IA y adoptar medidas técnicas y organizativas necesarias para asegurar su uso adecuado.

2

Supervisión humana: establecer una supervisión mediante la delegación a personas con la competencia, formación y autoridad requeridas.

3

Obligaciones legales nacionales: observar las obligaciones que otras disposiciones adicionales de la UE o los Estados Miembros de la UE establezcan.

4

Datos de entrada: asegurar que los datos de entrada sean relevantes y representativos para el propósito del sistema de IA.

5

Vigilancia y reporte: monitorear el sistema de IA y reportar cualquier riesgo o incidente grave al proveedor y autoridades pertinentes.

6

Conservación de registros: mantener archivos de registro generados automáticamente por un período mínimo de seis meses.

7

Información a empleados: informar a trabajadores y sus representantes antes de usar sistemas de IA de alto riesgo en el lugar de trabajo.

8

Registro: las Autoridades públicas y de la Unión deben cumplir con las obligaciones de registro sistema de alto riesgo en la base de datos de la UE y no usar sistemas no registrados en la citada base de datos.

9

Evaluación de impacto de protección de datos: realizar una evaluación de impacto de protección de datos, según lo requerido por la legislación aplicable de protección de datos.

10

Información sobre decisiones: informar a las personas físicas cuando estén expuestas a decisiones tomadas con ayuda de IA de alto riesgo.

11

Cooperación con autoridades: colaborar con las autoridades nacionales competentes.

12

Evaluación de impacto de derechos fundamentales: evaluar el impacto en los derechos fundamentales, incluyendo:

- Descripción de cómo se usará el sistema IA.
- Detallar el tiempo y la frecuencia de uso.
- Identificar a las personas y grupos afectados.
- Evaluar los riesgos específicos para estas personas y grupos afectados.
- Describir las medidas de supervisión humana aplicadas.
- Planificar acciones en caso de que los riesgos identificados ocurran.

Si hay cambios significativos durante el uso del sistema, la evaluación debe actualizarse. Los resultados de la evaluación deben ser notificados a la autoridad de vigilancia del mercado.

## Riesgo medio

El **Reglamento IA** establece las siguientes cuestiones para sistemas de IA que se consideran de riesgo medio:

1

**Los sistemas de IA que interactúan con personas** deben informarles de que están interactuando con IA, a menos que sea obvio o estén autorizados por ley para asuntos penales.

2

**Los sistemas de IA que crean contenido sintético** deben marcarlo para que se identifique como artificial.

3

**Los sistemas de reconocimiento de emociones o categorización biométrica** deben informar a las personas sobre su funcionamiento y cumplir con la regulación de datos.

4

**Los sistemas de IA que generen ultrafalsificaciones (deep fakes)** deben revelar que el contenido es artificial.

## Riesgo limitado

Los sistemas de IA que no generan riesgos, tales como sistemas o filtros antispam o sistemas de IA utilizados en videojuegos no están sujetos a requisitos establecidos por el Reglamento IA.

# Modelos y sistemas de IA de uso general



Se considera que los modelos de IA de uso general tienen riesgo sistémico cuando están dotados de **capacidades de gran impacto** o aquellos en los que **la cantidad acumulada de cálculo utilizada para su entrenamiento sea superior a  $10^{25}$** , medida en número de operaciones de coma flotante (FLOP).

El Reglamento IA considera que este tipo de modelos son **susceptibles de dar lugar a usos que puedan implicar riesgos inaceptables con mayor facilidad** que otro tipo de sistemas, por lo que se establecen las siguientes obligaciones específicas:

- realizar la evaluación del modelo;
- evaluar y reducir los riesgos sistémicos a escala de la UE;
- vigilar, documentar y comunicar los incidentes graves y las medidas correctoras a la Oficina de IA y a las autoridades nacionales competentes
- y garantizar un nivel adecuado de protección de la ciberseguridad.

El Reglamento IA establece que la Oficina de IA fomentará y facilitará la elaboración de **códigos de buenas prácticas** y podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los mismos.

# Espacios controlados de pruebas (sandbox)



En su ánimo de fomentar la innovación, el Reglamento IA fomenta el establecimiento de espacios controlados de pruebas para la IA con el propósito de conectar a las autoridades competentes con las compañías desarrolladoras de inteligencia artificial.

Los sandbox persiguen los siguientes **objetivos**:

- definir, de forma conjunta, buenas prácticas de aplicación del Reglamento IA;
- facilitar el desarrollo de un ecosistema IA;
- contribuir a un aprendizaje regulatorio;
- facilitar y acelerar el acceso al mercado de sistemas IA, sobre todo de pymes y startups.



A nivel europeo, España es el primer país en establecer un sandbox regulatorio sobre IA.

# Gobernanza del Reglamento IA y sanciones



Qualentum Lab

Tanto la Comisión Europea como los Estados Miembros de la UE tienen responsabilidades distintas en la aplicación del Reglamento IA.

En el ámbito de la UE, la Comisión ha creado dos entidades:

## **La Oficina de IA**

Responsable de desarrollar los conocimientos especializados y las capacidades de la UE en el ámbito de la IA.

## **El Comité Europeo de Inteligencia Artificial**

Compuesto por un representante de cada Estado Miembro y por el Supervisor Europeo de Protección de Datos en calidad de observador. La función del Comité Europeo de Inteligencia Artificial es prestar asesoramiento y asistencia a la Comisión Europea y a los Estados miembros para facilitar la aplicación coherente y eficaz del Reglamento IA.

Por su parte, cada Estado miembro debe establecer:

- una **autoridad notificante**, responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de conformidad
  - y una **autoridad de vigilancia** del mercado, que debe velar por el cumplimiento del Reglamento IA en su respectivo territorio.
- 

**En España, la AESIA (Agencia Española de Supervisión de la Inteligencia Artificial) ha asumido este papel. En todo caso, estas Autoridades deben disponer de recursos adecuados para desarrollar su función y en un régimen de independencia y autonomía, a fin de evitar conflictos de intereses.**

## Sanciones

Respecto de las potenciales sanciones en casos de incumplimiento, el Reglamento IA prevé altas sanciones, que pueden llegar **hasta 35 millones de euros o el 7% del volumen de negocios mundial anual**, lo cual da muestra de la importancia del cumplimiento con el Reglamento IA.

# Entrada en vigor y periodo de transición



El Reglamento IA se publicó el 12 de julio de 2024 en el Diario Oficial de la Unión Europea y entró en vigor el 1 de agosto de 2024. No obstante, y a fin de conceder un plazo de adaptación, algunas disposiciones contenidas no serán aplicables en las siguientes fechas.

- Las prohibiciones por riesgo inaceptable (usos prohibidos) se aplicarán **6 meses después desde la entrada en vigor** (2 de febrero de 2025).
- Las disposiciones aplicables a los **modelos y sistemas de uso general** ya comercializados serán aplicables a los **12 meses desde la entrada en vigor** (2 de agosto de 2025).
- Aplicación general del Reglamento IA: **2 de agosto de 2026** (incluido Anexo III).
- Las obligaciones relativas a **sistemas de alto riesgo para productos o componentes de seguridad (Anexo I Reglamento)** serán aplicables a los **36 meses desde la entrada en vigor**.

# Conclusión



Como ya ocurrió hace algunos años con el marco en materia de la protección de datos personales (Reglamento General de Protección de Datos de la UE), el Reglamento IA representa un marco normativo de referencia en la Unión Europea y en el resto del mundo. En él se establecen las obligaciones para todos los intervenientes en la cadena de valor de la IA, y debemos conocer todas ellas en detalle para evitar consecuencias indeseadas o altas sanciones en casos de incumplimiento.

Asimismo, como hemos visto, el Reglamento IA establece un equilibrio entre el impulso a la innovación a través de los espacios controlados de pruebas o exenciones de aplicación, así como un marco robusto para la protección de las personas y de los valores de la Unión Europea.

¡Enhорabuena! Fastbook superado



[Qualentum.com](http://Qualentum.com)