

A blurred background image of a modern office interior. Several people are visible, some sitting at desks with laptops, others standing. The image is out of focus, creating a sense of motion and activity. The text is overlaid on this background.

Marco Legal Europeo para el **Uso Responsable de la IA**

íFounderz



Reglamento de Inteligencia Artificial

Marco Legal Europeo para el Uso Responsable de la IA

Hoy en día, la Inteligencia Artificial se ha convertido en parte del día a día de empresas y profesionales. Ya sea de manera más informal o en procesos clave del trabajo, su uso es una realidad que crece sin parar.

Este avance, aunque ofrece grandes beneficios, también abre la puerta a riesgos y dilemas que necesitan ser regulados.

Con este objetivo, de proteger a empresas, empleados y consumidores, la Unión Europea ha impulsado la creación de un reglamento específico que dé respuesta a los retos de esta nueva era.

¿Qué es el Reglamento de Inteligencia Artificial (RIA)?

Marco legal común



Establece normas unificadas en la UE para garantizar que el desarrollo, uso y comercialización de la IA sea **seguro, ético y fiable**.

Aplicación progresiva



Aprobado en 2024, aplica de forma gradual hasta su **implementación completa en agosto de 2027**.

Responsabilidades diferenciadas



Regula obligaciones específicas para cada actor: **proveedores, integradores y usuarios de IA**.

El RIA define cuatro pilares fundamentales:

Usos prohibidos de la IA

Prácticas que vulneran derechos fundamentales están completamente vetadas.

Obligaciones para IA de alto riesgo

Sistemas que impactan en áreas críticas requieren controles estrictos.

Transparencia en IA de uso general

Modelos como GPT deben cumplir requisitos de transparencia específicos.

Alfabetización en IA

Obligación de formar a usuarios en el uso responsable de la tecnología.

En definitiva, la entrada en vigor del RIA puede implicar, tanto para empresas e individuos que hagan un uso profesional de la IA, nuevas obligaciones de transparencia, control de calidad, documentación técnica y supervisión humana, lo que impacta directamente en el diseño, comercialización y uso de soluciones basadas en IA.



Objetivos de la regulación



Proteger derechos fundamentales

La IA no puede poner en riesgo la privacidad, la igualdad o la dignidad de las personas. El objetivo es **evitar usos que puedan discriminarnos o manipularnos.**



Generar confianza en el uso de la IA

Para que las empresas y ciudadanos adopten la IA, necesitamos **transparencia, responsabilidad y sistemas seguros** que respeten nuestros valores.



Evitar fragmentación normativa

El RIA es único para todos los países de la Unión Europea. Así se evitan leyes diferentes en cada estado y **se facilita la circulación de productos y servicios de IA.**



Impulsar competitividad e innovación

El Reglamento busca dar seguridad jurídica a las empresas y favorecer la innovación, permitiendo que Europa lidere el desarrollo de **soluciones de IA confiables.**

En esencia, este Reglamento busca que la IA sea **segura, ética y beneficiosa para todos.**

Niveles de riesgo en IA

El RIA no impone los mismos requisitos a todas las IAs, sino que establece cuatro niveles diferenciados:



Clave: Debemos identificar claramente ante qué nivel de riesgo nos encontramos para implementar las medidas correspondientes.

Alfabetización en Inteligencia Artificial

Considerando el impacto que la IA tiene en la forma en la que trabajamos, aprendemos y tomamos decisiones, el RIA obliga a los individuos y empresas a formar a sus equipos en materia de Inteligencia Artificial.

Qué es la IA y cómo funciona

Por ejemplo, cómo un modelo como GPT es capaz de generar un resumen de un informe.

Conocer los tipos de IA

No es lo mismo un modelo de uso general que un sistema de alto riesgo que evalúa candidatos.

Entender los riesgos

La IA puede equivocarse, reproducir sesgos o vulnerar la privacidad si no se usa bien.

Aplicar buenas prácticas

Ser transparentes, supervisar resultados y avisar cuando el contenido fue generado con IA.

No solo se trata de cumplir con la ley, sino que entender cómo funciona la IA, sus riesgos y sus límites, es clave para usarla de forma [ética, segura y eficaz](#).

¿Quién debe recibir formación?



Todos los empleados

Que usen IA en su trabajo, **desde administrativos hasta desarrolladores.**



Responsables de implementación

De **soluciones de IA** en la organización.



Directivos y mandos internos

Que toman **decisiones estratégicas sobre IA.**



Equipos de producto y marketing

Que integren modelos como **GPT, Claude y similares.**

La formación debe ser **integral y continua**, adaptándose a los roles específicos de cada profesional.

Alfabetización en Inteligencia Artificial

Considerando el impacto que la IA tiene en la forma en la que trabajamos, aprendemos y tomamos decisiones, el RIA obliga a los individuos y empresas a formar a sus equipos en materia de Inteligencia Artificial.

No solo se trata de cumplir con la ley, sino que, entender cómo funciona la IA, sus riesgos y sus límites, es clave para usarla de forma [ética](#), [segura](#) y [eficaz](#).

Estar alfabetizados en IA implica tener claro:



Qué es la IA y cómo funciona

Por ejemplo, cómo un modelo como GPT es capaz de generar un resumen de un informe.



Conocer los tipos de IA

No es lo mismo un modelo de uso general, como los asistentes virtuales, que un sistema de alto riesgo, aquellos que evalúan candidatos o gestionan datos sensibles.



Entender los riesgos

La IA puede equivocarse, reproducir sesgos o vulnerar la privacidad si no se usa bien.

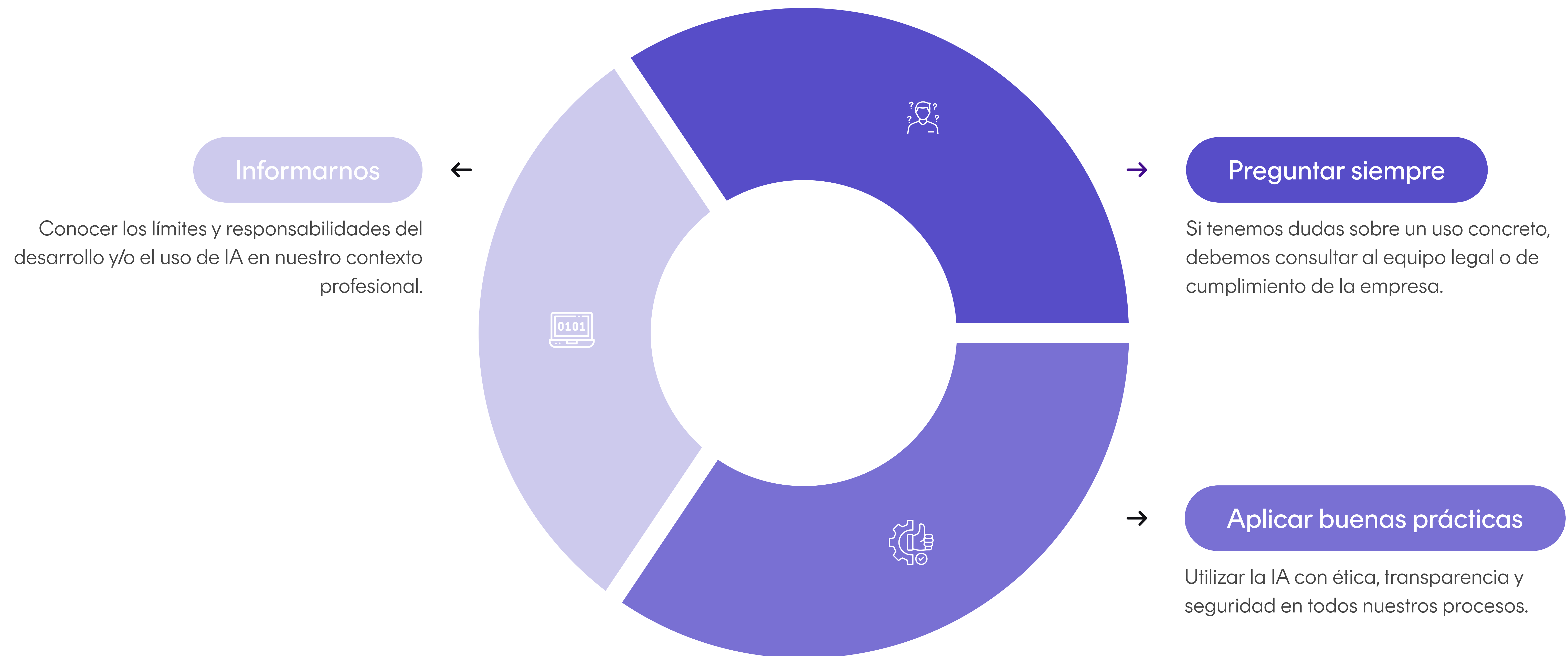


Aplicar buenas prácticas

Ser transparentes, supervisar siempre los resultados y, cuando corresponde, avisar si un texto, una imagen o un vídeo, fueron generados con IA.



Responsabilidades principales



El uso responsable de la IA es una [responsabilidad compartida](#) que requiere compromiso de toda la organización.

Prácticas prohibidas en IA

La Inteligencia Artificial es una gran aliada en nuestro trabajo pero no todo vale. El RIA establece límites claros para proteger la privacidad, la igualdad y los derechos fundamentales.

Manipulación subliminal

Usar IA para influir en las decisiones de una persona sin que lo sepa (por ejemplo, forzando compras, ocultando información).

Explotación de vulnerabilidades

Aprovecharse de la edad, discapacidad o situación social (por ejemplo, crear apps que inciten a menores a comprar productos).

Social scoring

Clasificar personas según su comportamiento para dar o negar servicios (por ejemplo, un banco que puntúa clientes según su historial online).

Reconocimiento biométrico masivo

Uso de bases de datos biométricas sin consentimiento (por ejemplo, reconocimiento facial en centros comerciales).

Detección de emociones

En el trabajo o sector educativo (por ejemplo, analizar expresiones faciales de empleados para medir motivación).



Advertencia: Infringir estas normas puede suponer **multas millonarias** y un daño reputacional irreparable para las empresas.

Impacto en obligaciones clave

Cuando usamos IA, podemos estar **gestionando datos, información sensible y contenido protegido**. Entender estas implicaciones nos ayuda a proteger la empresa, a los clientes y a nosotros mismos.

Confidencialidad

Protección de información sensible y datos empresariales.

Propiedad intelectual

Derechos sobre contenidos y resultados generados.

Datos personales

Cumplimiento de normativas de protección de datos.

Seguridad

Protección contra ciberataques y vulnerabilidades.

Estas cuatro áreas requieren **atención especial** en cualquier implementación de IA empresarial.

Confidencialidad y propiedad intelectual

→ Confidencialidad

La IA suele procesar grandes volúmenes de información, y parte de ella puede ser sensible: datos de clientes, estrategias de negocio o contratos.



Ejemplo de riesgo: Subir contratos a un chatbot público como ChatGPT puede exponer información confidencial a terceros.

Es fundamental respetar la política interna de gestión de la información aprobada por la empresa.

→ Propiedad intelectual

- 1. Entrenamiento de IA:** Algunos modelos se entrenan con contenidos protegidos por derechos de autor sin licencia adecuada.
- 2. Titularidad de resultados:** Debe confirmarse quién es el propietario de los contenidos generados por IA.

Antes de usar cualquier resultado públicamente, [revisa siempre las condiciones de la herramienta](#).

Datos personales y seguridad

1

Datos personales

La IA debe cumplir la normativa de protección de datos: se debe informar, limitar y justificar el tratamiento con una base legal.



Ejemplo de incumplimiento: introducir un prompt en un chatbot con datos personales de un cliente para generar un informe.

Nunca introduzcas información personal en sistemas de IA no autorizados.

2

Seguridad

La IA también puede ser atacada. Un ciberataque podría alterar el sistema de IA que gestiona inventarios, provocando pedidos incorrectos o retrasos en la cadena de suministro.

Debemos cumplir las políticas internas de seguridad y **reportar cualquier incidente sospechoso**.

3

La protección de datos y la seguridad son **pilares fundamentales** en el uso responsable de IA.

Régimen sancionador

El RIA establece multas importantes si no cumplimos la normativa. Desde el 2 de agosto de 2025, las autoridades europeas podrán sancionar con:

35M€

Prácticas prohibidas

Hasta 35 millones de euros o el 7% de la facturación global.

15M€

Incumplimiento de obligaciones

Hasta 15 millones o el 3% de la facturación global.

7.5M€

Información incorrecta

Hasta 7,5 millones o el 1% de la facturación global.

Fechas clave a recordar

Agosto 2025

Inicio de sanciones por prácticas prohibidas.

1

Agosto 2026

Sanciones para IA de alto riesgo.

2

Agosto 2027

Cumplimiento total para modelos de uso general.

3



La IA es poderosa, pero su uso responsable depende de todos nosotros.

Formarnos, proteger los datos y cumplir con la normativa es la clave para aprovechar todo su potencial de forma segura, ética y legal.

Founderz