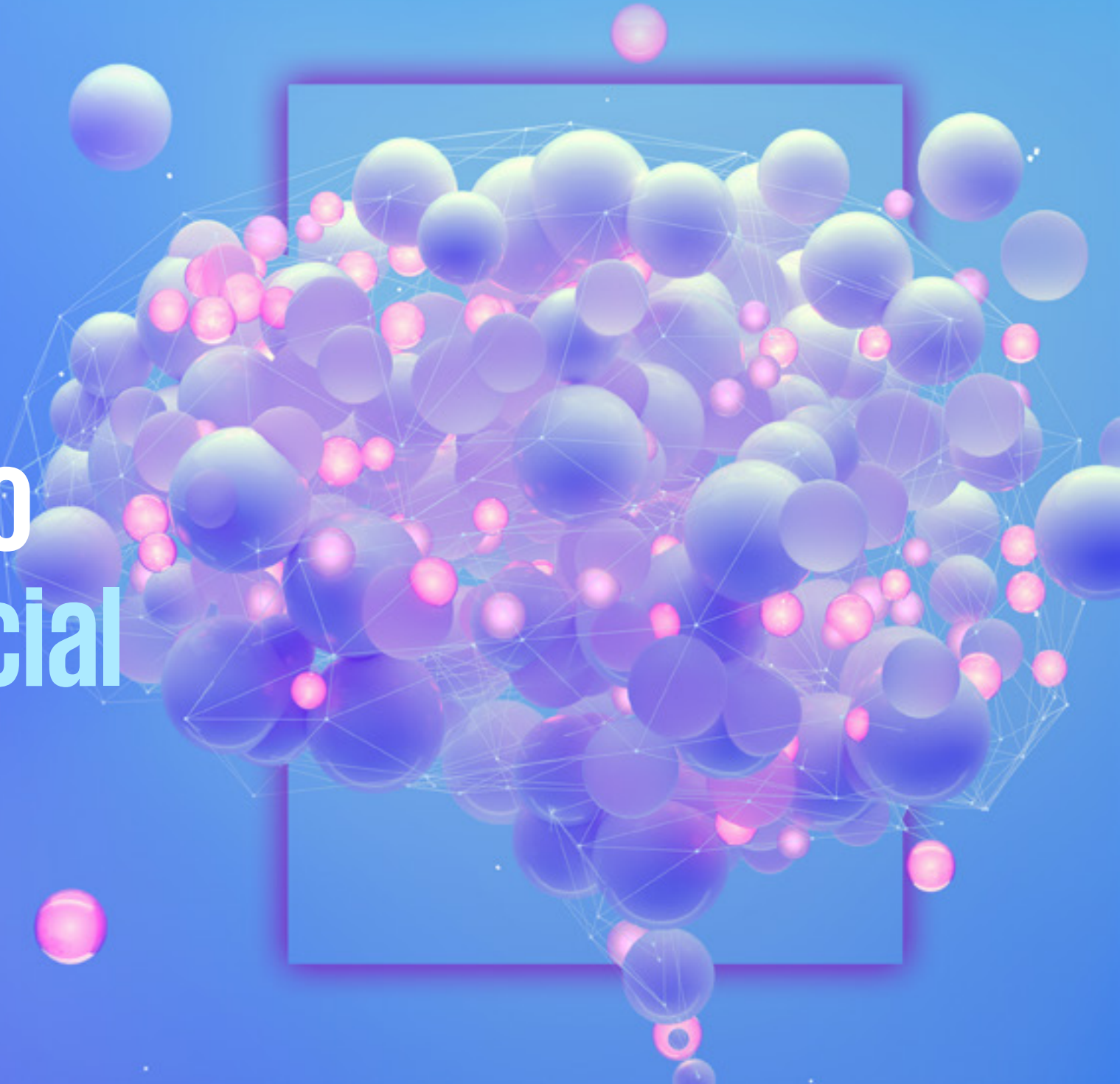




Aspectos clave para entender la primera regulación del mundo de Inteligencia Artificial

KPMG. Make the Difference.



La Unión Europea se ha convertido en la primera región del mundo en contar con un marco jurídico transversal y uniforme para el desarrollo confiable de la inteligencia artificial (IA). Es el conocido Reglamento europeo de Inteligencia Artificial (RIA), cuyo gran objetivo es, a partir de un enfoque basado en riesgos, proteger los derechos fundamentales de las personas, entre otros riesgos, ante la llegada de una tecnología que impacta fuertemente en la sociedad y la economía.

Se trata de un reto mayúsculo para las empresas, ante el que surgen grandes interrogantes: ¿Que preguntas deben hacerse las organizaciones? ¿Qué obligaciones tienen en función del riesgo de cada sistema? ¿A qué sanciones se exponen por incumplirlas?

Descubre las respuestas a continuación.

Objetivos



Reglamento,
de aplicación
directa en la
Unión Europea



¿Qué es una IA?

Un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y 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 resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

** A estos efectos, es muy importante considerar las distintas tipologías de datos definidos también en el RIA (datos de entrada, datos de entrenamiento, datos de validación, o los datos de prueba)*

Ejemplos:



Asistentes virtuales inteligentes (Siri, Alexa, Cortana...)



Sistemas de reconocimiento facial (FaceID de Apple)



Traductores simultáneos (Google Translate)



Sistemas de recomendación en plataformas de contenido

¿Cómo deben responder las organizaciones?

Pasos a seguir:

1

¿Tenemos un sistema IA?

2

¿Qué tipo de IA?

Es necesario categorizarlo:

RIESGO INACEPTABLE



En esta categoría se incluyen aquellos sistemas de IA que representan una amenaza directa a la seguridad pública, los derechos fundamentales o la privacidad. Su uso está estrictamente prohibido, salvo en situaciones muy excepcionales. Hablamos de sistemas caracterizados por:

- Manipular cognitivamente el comportamiento de personas.
- Manipular el comportamiento que aprovecha vulnerabilidades de personas o grupos concretos.
- Evaluar o puntuar socialmente.
- Identificar biométricamente en tiempo real en espacios públicos.

RIESGO ALTO



Aquí se incluyen los sistemas de IA que podrían tener un impacto considerable en los derechos fundamentales de los individuos por su relación con los servicios y procesos que afectan a la salud, seguridad, etc. Su uso está permitido siempre que se cumplan con ciertas salvaguardas adicionales y se monitorice su funcionamiento. Esta categoría engloba a sistemas que cumplen estas dos condiciones:

Condición 1

- Están destinados a utilizarse como componente de seguridad de un producto.
- Deben someterse a una evaluación de conformidad por terceros con vistas a la comercialización o puesta en servicio del producto.

Condición 2

O, por otra parte, sistemas específicos recogidos en el Anexo III del Reglamento, cuando influyen en la toma de decisiones que puedan suponer un riesgo sobre la salud, la seguridad o los derechos fundamentales.

Recomendación:

Se recomienda revisar en cada momento si el sistema de IA puede ser catalogado como de riesgo alto dado que la tipología de casos puede cambiar en el tiempo.

RIESGO LIMITADO



En este nivel se clasifican sistemas con algunas obligaciones concretas de transparencia:

- Sistemas de reconocimiento de emociones o que determinen la asociación a categorías sociales concretas a partir de datos biométricos.
- Sistemas que manipulan contenido (imagen, sonido, vídeo, ...) que asemeje a personas, objetos, lugares e entidades y puedan inducir erróneamente a una persona a pensar que son auténticos o verídicos.



Modelos de IA de propósito general (con o sin riesgo sistémico)

Sistema que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado.

Los modelos de IA de uso general que no presenten riesgos sistémicos están sujetos a algunos requisitos limitados, por ejemplo, con respecto a la transparencia, pero aquellos con riesgos sistémicos tendrán que cumplir con reglas más estrictas.

3

Demostrar la existencia de una gobernanza y diligencia debida en el control de tales riesgos, procurando la existencia de **un modelo responsable y confiable en IA.**

4

RIESGO ALTO



En caso de tratarse de un sistema de riesgo alto, la compañía deberá **registrarlo**

En todo caso, es necesario crear una cultura en la que todas las partes involucradas (empleados, clientes, terceros externos) entiendan los riesgos asociados a los sistemas conforme a los marcos de gobernanza que se establezcan, impulsando la alfabetización en IA (formación y concienciación) al respecto.

Obligaciones específicas para los sistemas de

ALTO RIESGO



Implantación de un sistema de gestión de riesgos y calidad

Gobernanza de datos

Transparencia y comunicación de información a los responsables del despliegue

Supervisión humana

Precisión, solidez y ciberseguridad

Evaluación de impacto sobre los derechos fundamentales y evaluación de conformidad

Establecer y mantener la documentación técnica asociada a un sistema de IA de alto riesgo

Se permitirá técnicamente el registro automático de acontecimientos y la trazabilidad a lo largo de todo el ciclo de vida del sistema

Ejemplos:



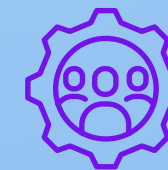
Sistemas de verificación de la autenticidad de los documentos de viaje



Dispositivo médico: un robot de cirugía supervisada por una IA



Sistemas que arrojen una puntuación de crédito que impide la obtención de un préstamo



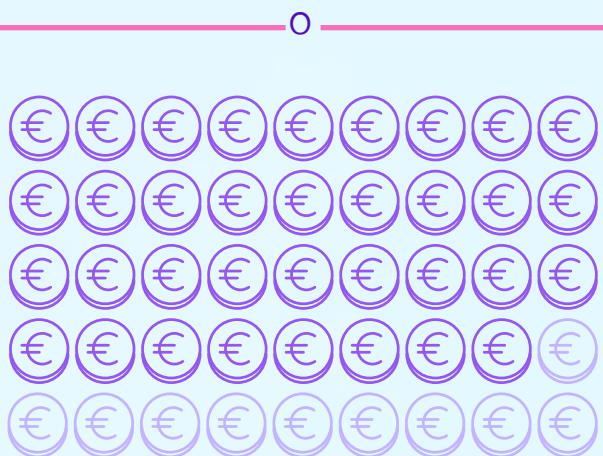
Sistemas de selección de personal

Sanciones en caso de incumplimiento

RIESGO ALTO

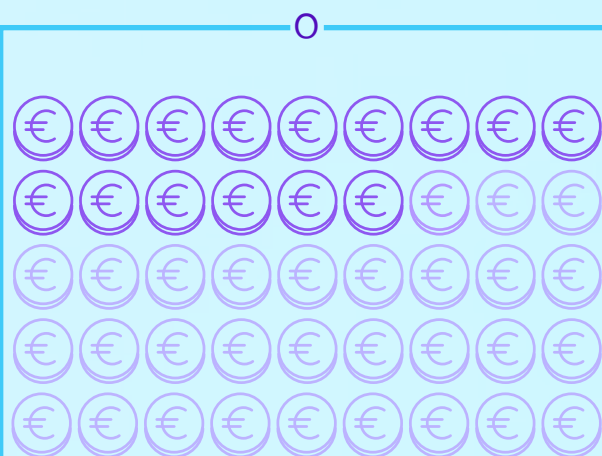


Hasta el **7%** de la facturación anual global



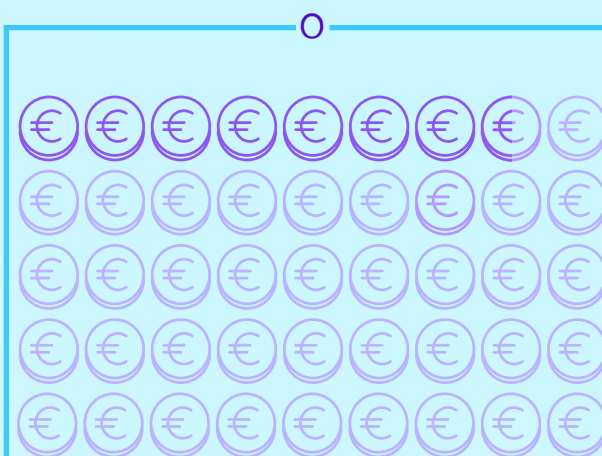
35 millones de euros en caso de sistemas de IA prohibidos

Hasta el **3%** de la facturación anual global



15 millones de euros para la mayoría de las demás infracciones

Hasta el **1%** de la facturación anual global

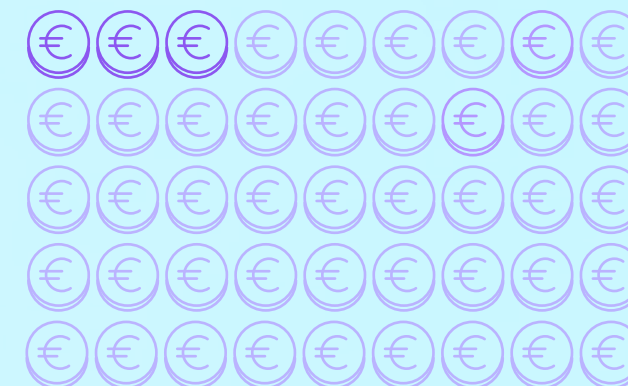


7,5 millones de euros por suministrar información inexacta, incompleta o engañosa

PYMES

Cada una de las multas podrá ser por el porcentaje o el importe al que se refiere en los apartados anteriores según cual de ellos sea menor

La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen



3% de su volumen de facturación anual global

Próximos pasos

Tras ser firmado por los presidentes del Parlamento Europeo y del Consejo, el acto legislativo se publicará en el Diario Oficial de la UE en los próximos días y entrará en vigor veinte días después de esta publicación. El nuevo reglamento se aplicará dos años después de su entrada en vigor, con algunas excepciones para disposiciones específicas de las fechas en las que resultan aplicables las diferentes disposiciones del Reglamento.

6 meses

Disposiciones sobre IA prohibidas de riesgo inaceptable



12 meses

Disposiciones sobre autoridades competentes de los Estados miembros y modelos de IA de propósito general



24 meses

Obligaciones correspondientes a determinados sistemas de IA de alto riesgo

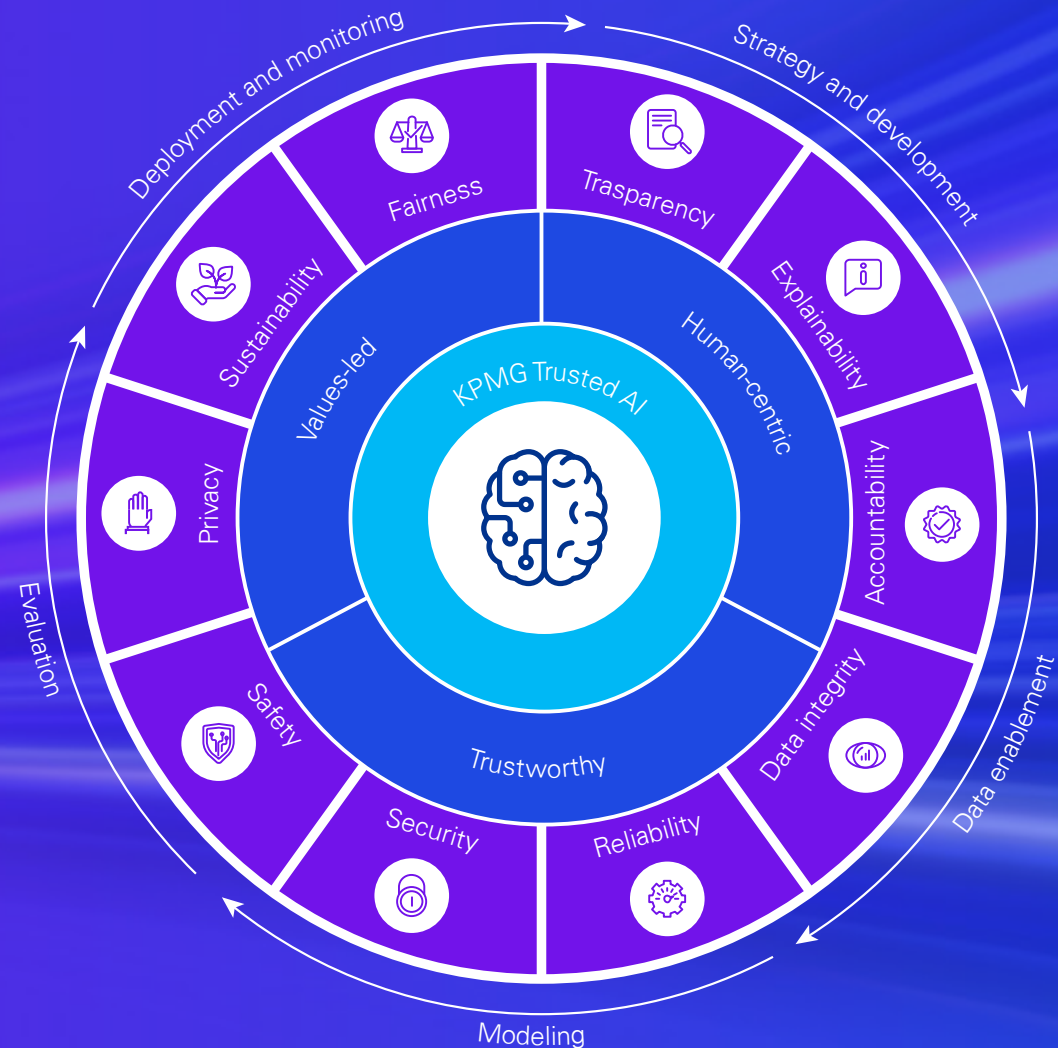
Cómo puede ayudarte KPMG

Para abordar y cumplir con la nueva regulación, compartimos nuestros principios, pilares éticos y aproximación al gobierno en materia de Inteligencia Artificial.

KPMG Trusted AI es nuestro enfoque estratégico y marco para diseñar, construir, desplegar y utilizar soluciones de IA de manera responsable y ética, con el objetivo de acelerar la creación de valor con confianza.

Las capacidades de la IA están evolucionando rápidamente y por tanto, también nuestro enfoque con especial atención a las obligaciones específicas asociadas a IA Generativa (GenAI).

A medida que los avances tecnológicos y los estándares legales, éticos, y de riesgos maduren, KPMG continuará revisando y evolucionando nuestro marco de **Trusted AI** y servicios asociados como sea necesario.





La transformación nunca para. Nosotros tampoco.

En KPMG creemos que la transformación es una oportunidad que no se puede dejar pasar. Integrando la mejor tecnología, con los procesos adecuados y las capacidades y visión necesarias, la transformación será un éxito. Por esa razón, hemos trabajado durante décadas en el corazón de las empresas, ayudando a nuestros clientes a maximizar el potencial de sus personas y de su tecnología, trabajando junto para alcanzar resultados reales. Porque cuando personas y tecnologías se unen, el resultado es insuperable.

Construyendo un mundo diferente:

Los profesionales de KPMG marcan la diferencia en la transformación tecnológica de tu organización. Juntos, te ayudamos a orientar tu negocio al cliente, optimizar funciones para afrontar nuevos retos, gestionar los riesgos y la regulación, alcanzar nuevas cotas de generación de valor y crear un entorno para adaptarse a los cambios.

KPMG. Make the Difference.



Contactos

Javier Aznar
Socio de **Technology Risk**
de **KPMG en España**
E: jaznar@kpmg.es
T: +34 699 35 00 29

Noemí Brito
Socia responsable del área de 'Legal
Operations & Transformation Services
(LOTS) y de **IP & IT de KPMG Abogados**
E: noemibrito@kpmg.es
T: +34 689 38 57 98

Eva García
Socia responsable de **Análisis de Datos e**
Inteligencia Artificial de KPMG en España
E: evagarcia1@kpmg.es
T: +34 685 94 88 10

**Te ayudamos a sacar el máximo partido al despliegue
de la inteligencia artificial generativa en tu organización**

Descubre cómo

kpmg.es

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.

© 2024 KPMG, S.A., sociedad anónima española y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Limited, sociedad inglesa limitada por garantía.