

Juego limpio: la importancia del Compliance en el ámbito empresarial desde una perspectiva internacional

Almudena Curero

Associate Partner Legal Compliance

30 de septiembre de 2026

—

kpmg.es

Índice

01

Introducción. La importancia creciente del *Compliance*.

02

La evolución de los modelos de *Compliance*. *Compliance* de tercera generación.

03

Principales retos de la Inteligencia Artificial en *Compliance*.

04

La regulación europea sobre el uso ético de la IA.

Introducción. La importancia creciente del *Compliance*

01

Más reglas, más interdependencia y más exposición

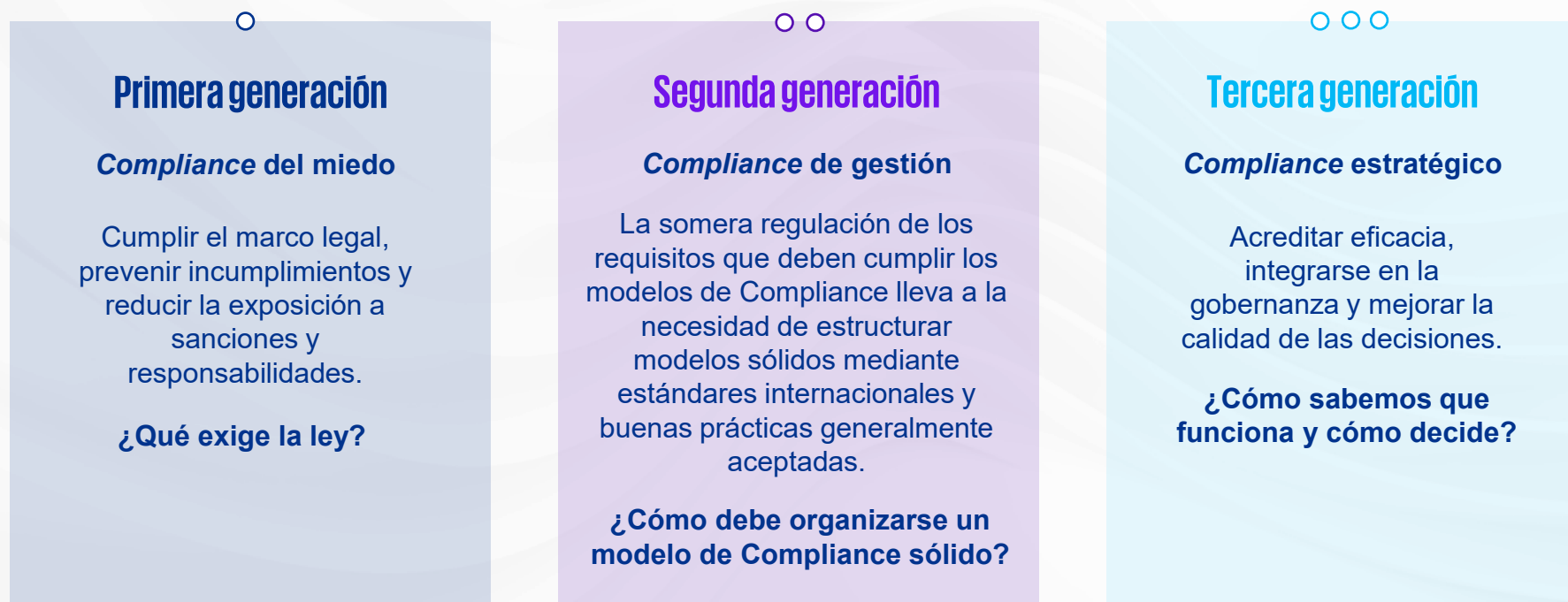


**La evolución de los
modelos de *Compliance*.
Compliance de tercera
generación.**

02

Tres generaciones, tres centros de gravedad

El modelo evoluciona conforme se hacen más exigentes las preguntas que debe responder.



No estamos ante tres etapas estancas ni ante una sucesión de modelos que se sustituyen unos a otros. Cada generación conserva los elementos valiosos de la anterior, pero incorpora una nueva exigencia que desplaza el centro de gravedad del modelo.

Primera generación: El *Compliance* del miedo

La primera generación surge como respuesta a una preocupación esencialmente jurídica y sancionadora.

La expansión de la responsabilidad corporativa y la creciente capacidad de actuación de reguladores y autoridades convierten el *Compliance* en un mecanismo de protección frente al incumplimiento.

Su finalidad prioritaria es identificar qué exige la ley, implantar los elementos de prevención necesarios y acreditar la diligencia de la organización. El éxito tiende a asociarse a la ausencia de infracciones, sanciones o incidentes.

Se configura así un modelo predominantemente defensivo: imprescindible para reducir la exposición, pero todavía centrado en controlar conductas y documentar la respuesta organizativa.

El *Compliance* se concibe, ante todo, como una barrera frente al riesgo legal.

La lógica dominante es preventiva y defensiva

- Cumplimiento del marco legal.
- Prevención de incumplimientos.
- Reducción de sanciones y responsabilidades.
- Políticas, controles y evidencia documental.

Segunda generación: El *Compliance* de gestión

De los elementos exigidos por la ley a una arquitectura organizativa sistemática.

La segunda generación aparece cuando las organizaciones comprenden que la mera existencia de políticas y controles no garantiza un modelo consistente. La regulación identifica sus componentes esenciales, pero suele ofrecer respuestas limitadas sobre cómo deben relacionarse, desplegarse, supervisarse y mejorarse.

Los estándares internacionales y las buenas prácticas aportan un lenguaje común y convierten la experiencia acumulada en marcos de gestión replicables, comparables y, en algunos casos, certificables.

El protagonismo pasa del control aislado al sistema: evaluación de riesgos, liderazgo, responsabilidades, recursos, formación, canales internos, investigaciones, seguimiento y mejora continua.

Normalizar no significa uniformar: significa disponer de referencias comunes para diseñar, comparar, supervisar y mejorar.

De los elementos exigidos por la ley a una arquitectura organizativa sistemática

- ISO 37301: gestión transversal.
- UNE 19601: Compliance penal.
- ISO 37001: antisoborno.
- ISO 37002 y 37008: canales e investigaciones.

Tercera Generación: El *Compliance* estratégico

De la existencia del modelo a la demostración de su eficacia y a la gobernanza de las decisiones

La tercera generación surge cuando la cuestión central deja de ser si el modelo existe o si está correctamente diseñado. La nueva exigencia consiste en demostrar que funciona, produce resultados y aprende de la experiencia. El foco se desplaza desde la actividad hacia el desempeño y desde la arquitectura formal hacia los cambios observables.

Al mismo tiempo, el *Compliance* se aproxima al espacio donde se originan las exposiciones más relevantes: la toma de decisiones. Su función no es sustituir al decisor, sino integrar información compleja, traducir obligaciones y expectativas en criterios útiles, aportar proporcionalidad y conservar evidencia de la diligencia aplicada.

La tecnología y la inteligencia artificial intensifican esta evolución, pero no la definen. El rasgo central es la capacidad de gobernar decisiones humanas y automatizadas cada vez más complejas.

El modelo maduro no es el que más controles acumula, sino el que puede explicar qué resultados produce, cómo influye en las decisiones y qué aprende.

De los elementos exigidos por la ley a una arquitectura organizativa sistemática

- Del diseño al desempeño.
- De la actividad a la evidencia de eficacia.
- Del control ex post a la participación temprana.
- De los controles a la gobernanza de decisiones.

Principales retos de la Inteligencia Artificial en Compliance

03

La IA convierte la tercera generación en una necesidad tangible

No añade únicamente obligaciones: cambia la escala, la velocidad y la profundidad del análisis de riesgos.

La IA no es solo un nuevo riesgo de *Compliance*. Es un detonante de la nueva generación de modelos de *Compliance*.

La tecnología amplía la capacidad de analizar información, reconocer patrones y preparar actuaciones.

Esa capacidad puede mejorar la prevención y la respuesta, pero también puede condicionar procesos relevantes antes de que una persona adopte la decisión final.

Compliance aporta valor, pero la decisión sigue siendo de los órganos de gobierno.

01

Más capacidad de análisis

La IA permite relacionar datos, señales y comportamientos que los controles convencionales no siempre captan de forma conjunta.

02

Más influencia sobre los procesos

Las recomendaciones, clasificaciones y actuaciones automatizadas pueden orientar el tratamiento posterior de una operación, una alerta o una comunicación.

03

Más exigencia de gobierno

Cuanto mayor es la autonomía y el impacto del sistema, mayor debe ser la claridad sobre sus límites, la supervisión humana y la responsabilidad final.

Surgen así dos retos: gobernar su uso y emplear la tecnología.

Dos retos inseparables: gobernar su uso y emplear la tecnología

La IA amplía la capacidad de análisis y gestión, pero exige límites éticos claros y sin desplazar el juicio profesional

El reto ya no consiste únicamente en determinar qué puede hacer la inteligencia artificial, sino en decidir qué debe hacer, bajo qué límites y con qué nivel de supervisión.

Ejemplo

El análisis de perfiles y operaciones de riesgo puede revelar señales de fraude o blanqueo, siempre mediante criterios transparentes, supervisables y sujetos a revisión humana. Pero no para detectar patrones de vulnerabilidad debe servir para proteger a las personas, no para incrementar su exposición.



Ejemplo

En el triaje de canales internos, un agente puede clasificar comunicaciones, resumir hechos relevantes, identificar información incompleta y proponer criterios iniciales de priorización o escalado. La valoración de los hechos, las actuaciones a adoptar y cualquier decisión que afecte a personas deben permanecer bajo supervisión humana efectiva.

La regulación europea sobre el uso de la IA

04

Tres modelos regulatorios: tres concepciones del riesgo y de la gobernanza

No existe una respuesta regulatoria neutra: cada modelo expresa una idea distinta sobre quién debe gobernar la tecnología y frente a qué riesgos debe responder.

01

ESTADOS UNIDOS

La IA como motor de innovación.

La ventaja competitiva depende de acelerar el desarrollo y la adopción.

- La intervención pública tiende a concentrarse en riesgos concretos y en sectores ya regulados
- La prioridad consiste en no frenar la inversión, la experimentación y el liderazgo tecnológico.

Gobernar la IA significa preservar el dinamismo del mercado sin ignorar sus impactos.

02

CHINA

La IA como infraestructura estratégica.

El Desarrollo tecnológico se integra en una estrategia de Estado.

- La regulación busca orientar la IA hacia los objetivos nacionales y preservar la estabilidad social.
- La seguridad, la soberanía tecnológica y el control de la información prevalecen frente a la autonomía del mercado.

Gobernar la IA significa conservar capacidad estatal de dirección y control.

03

UNIÓN EUROPEA

La IA como desafío de confianza.

La innovación necesita límites cuando puede afectar a personas y derechos.

- La intensidad de las obligaciones aumenta con el Riesgo para la salud, la seguridad y los derechos fundamentales.
- La empresa debe poder explicar el uso del Sistema, supervisor sus resultados y responder por sus impactos.

Gobernar la IA significa hacer compatibles innovación, protección y responsabilidad.

De una preocupación compartida a un marco jurídico común

La Unión Europea convierte su concepción de la IA como desafío de confianza en reglas comunes para todo el mercado interior.

Una respuesta común para un riesgo transfronterizo

La inteligencia artificial se desarrolla y circula a través de fronteras, sectores y cadenas de valor. Una proliferación de respuestas nacionales habría fragmentado el mercado interior y generado niveles distintos de protección.

La respuesta europea nace de la voluntad de establecer un marco común que permita desarrollar y utilizar la IA sin obstaculizar su circulación en la Unión y, al mismo tiempo, preservar la protección de datos, los derechos digitales y los principios éticos.

El objetivo no es elegir entre innovación y protección, sino crear las condiciones para que la innovación resulte confiable.

Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial

Qué es

El primer marco jurídico integral sobre inteligencia artificial, directamente aplicable en la Unión Europea.

Cuándo

Aprobado el 13 de junio de 2024, publicado el 12 de julio y en vigor desde el 1 de agosto de 2024.

¿Qué regula?

El desarrollo, la comercialización, la puesta en servicio y el uso de sistemas de IA, con obligaciones graduadas según el riesgo.

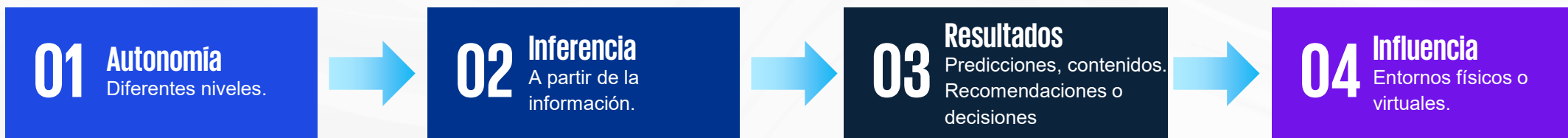


Qué entiende Europa por sistema de inteligencia artificial

La definición legal combina soporte tecnológico, autonomía, inferencia e influencia sobre entornos físicos o virtuales.

DEFINICIÓN DEL REGLAMENTO (UE) 2024/1689

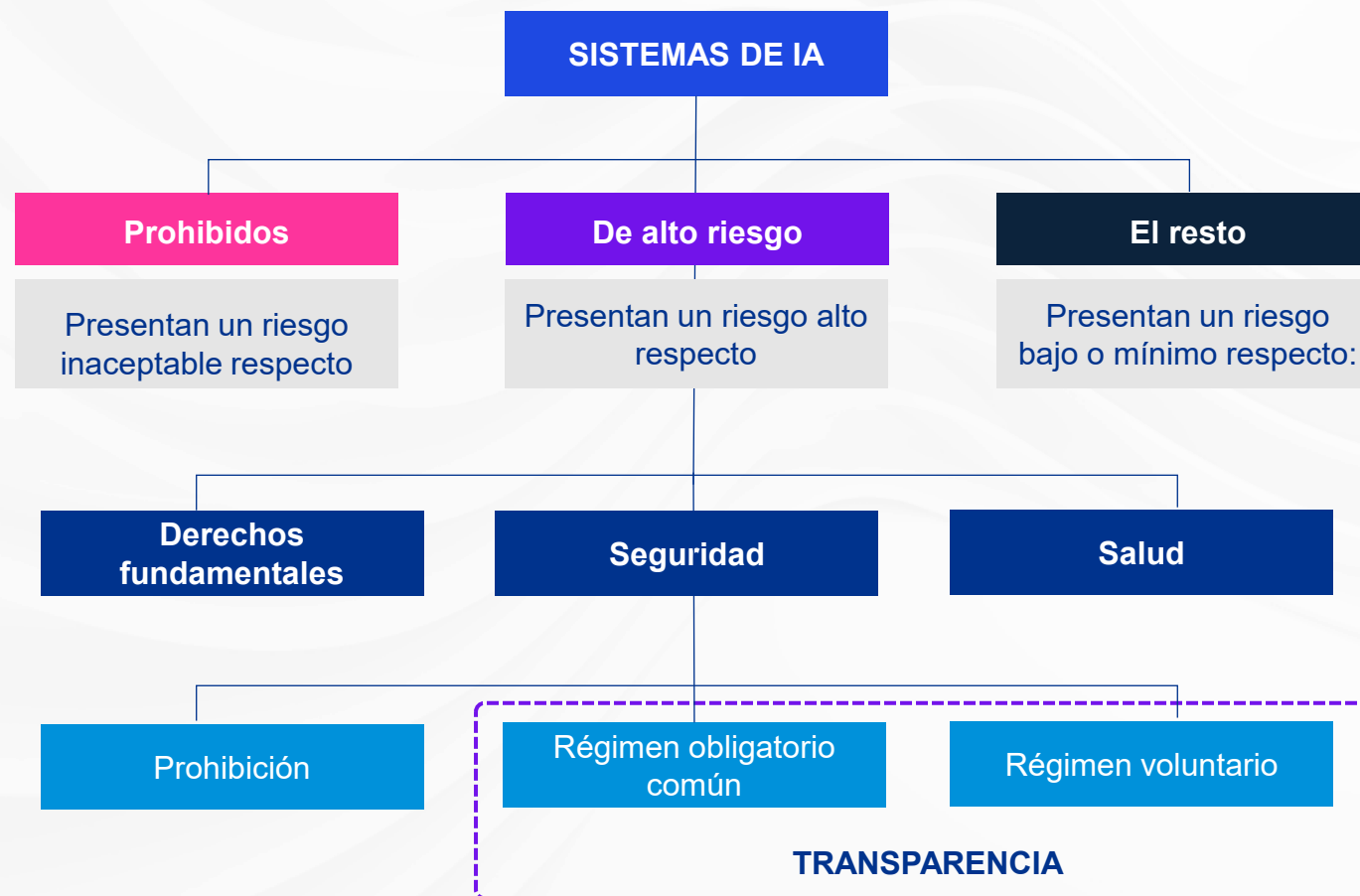
Sistema basado en una máquina diseñado para funcionar con diferentes niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue, y que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe, cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.



La definición no se limita a una técnica concreta: atiende a la capacidad del sistema para inferir y producir resultados con impacto.

Enfoque de protección de la UE

Clasificación de sistemas de IA según riesgo.



La transparencia opera frente a las personas y dentro de la organización

Informar de la intervención de la IA y poder reconstruir su funcionamiento son obligaciones distintas, pero complementarias.

Debe informarse de que se está interactuando con un sistema de IA cuando no resulte evidente y, en determinados supuestos, de que un contenido ha sido generado o manipulado artificialmente.CV

La persona puede comprender la naturaleza de la interacción y valorar su contexto.

FRENTE A LAS PERSONAS
Conocer cuándo interviene una IA

Lorem ipsum

FRENTE A LA ORGANIZACIÓN Y AL SUPERVISOR
Poder reconstruir cómo se produjo el resultado

Los procesos de actuación del sistema y sus resultados deben contar con la trazabilidad necesaria para auditar su corrección, identificar disfunciones y adoptar medidas correctoras.

La organización puede explicar, revisar y corregir la intervención del sistema.

La transparencia no consiste únicamente en informar de que existe IA, sino en poder explicar cómo ha intervenido y qué consecuencias ha producido.

Italia incorpora nuevos riesgos penales asociados al uso de la inteligencia artificial

Delitos relacionados con sistemas de IA incorporados al D.Lgs. 231/2001

15 SEP 2026

Publicación



30 SEP 2026

Entrada en vigor

El **D.Lgs. 160/2026** desarrolla la Ley italiana 132/2025 y adapta el ordenamiento italiano al Reglamento Europeo sobre Inteligencia Artificial en materia de responsabilidad civil, penal y responsabilidad de las entidades.

Introducción de dos nuevos delitos:

01

Art. 437-BIS Código Penal Italiano

OMISIÓN DE MEDIDAS DE SEGURIDAD Y ALTERACIÓN ILÍCITA

Protege frente a fallos, manipulaciones y ausencia de supervisión humana en sistemas de IA de alto riesgo.

02

Art. 612-QUATER Código Penal Italiano

DIFUSIÓN ILÍCITA DE CONTENIDOS GENERADOS O MANIPULADOS

Comprende la difusión ilícita de contenidos creados o alterados mediante IA, incluidos los deepfakes.

La regulación traslada obligaciones de seguridad, supervisión y uso responsable de la IA al ámbito penal y al sistema de responsabilidad de las entidades.

Italia incorpora nuevos riesgos penales asociados al uso de la inteligencia artificial

Ámbito del artículo 17 bis: sistemas de IA de alto riesgo

El delito de omisión de medidas de seguridad y alteración ilícita se aplica exclusivamente a sistemas de IA de alto riesgo y contempla tres conductas principales:

01 SEGURIDAD TÉCNICA

Omitir medidas para prevenir fallos o alteraciones durante el diseño, entrenamiento, producción o comercialización.

02 SUPERVISIÓN HUMANA

Omitir las medidas de supervisión humana exigibles, incluido el usuario profesional cuando actúa intencionadamente.

03 ALTERACIÓN ILÍCITA

Alterar el funcionamiento de un sistema de IA de alto riesgo cuando se genere el peligro exigido.

Es aplicable a cualquier entidad, empresa, organización o profesional que intervenga en el diseño, entrenamiento, producción, comercialización o utilización profesional de sistemas de IA de alto riesgo.

La conducta debe generar un peligro concreto para la vida, la integridad pública o individual, o la seguridad del Estado.

Su impacto en los modelos de Compliance

La incorporación de estos nuevos riesgos penales no sólo implica un mayor control tecnológico para las empresas, sino que requiere integrar la gobernanza de la IA en el modelo de Compliance, a través de las siguientes actividades:

**Inventario y
clasificación
de los sistemas
de IA**

**Evaluación de los
nuevos
riesgos penales**

**Medidas de
seguridad,
robustez y
resiliencia**

**Supervisión
humana
efectiva**

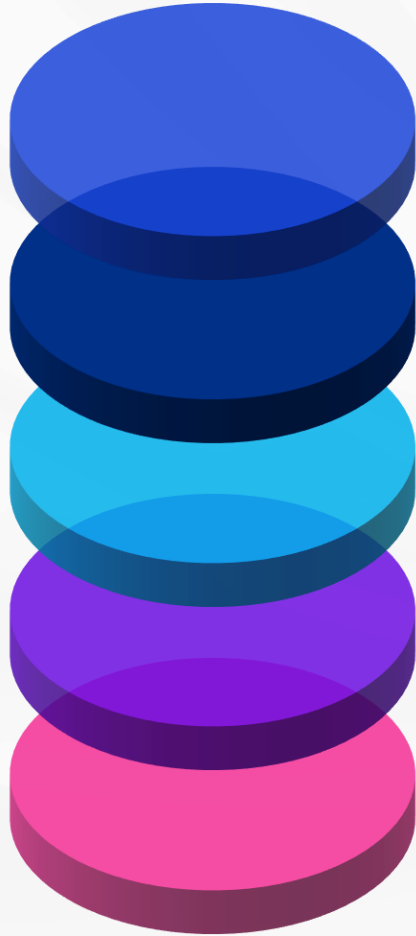
**Gobernanza,
funciones
y responsabilidades**

**Trazabilidad,
registros
y evidencia**

**Gestión de
proveedores
y terceros**

**Formación,
incidentes
y mejora continua**

Cinco ideas clave para concluir



01

La creciente interdependencia económica, tecnológica y regulatoria exige modelos de Compliance capaces de anticipar riesgos cada vez más sofisticados.

02

Los modelos de Compliance han transitado desde una lógica de prevención y control hacia una lógica de gobernanza y apoyo a la toma de decisiones.

03

La IA representa uno de los mayores desafíos actuales: no sólo introduce riesgos inéditos, sino que obliga a replantear cuestiones de responsabilidad, supervisión, trazabilidad y rendición de cuentas.

04

La gestión responsable de la IA exige incorporar consideraciones éticas, mecanismos de supervisión humana y salvaguardas destinadas a proteger derechos fundamentales y preservar la confianza

05

Los modelos de Compliance de tercera generación están llamados a desempeñar un papel esencial en la gobernanza de la IA.



Muchas gracias

Almudena Curero

Associate Partner

acurero@kpmg.es

Perfil de LinkedIn:

<https://www.linkedin.com/in/almudenacurero/>



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.

© 2026 KPMG Abogados S.L.P., sociedad española de responsabilidad limitada profesional 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.