

El uso de IA en las organizaciones: obligaciones reales, riesgos ocultos y exposición regulatoria



Prepararse para la adopción de IA

La empresa que despliega y utiliza la IA en su organización asume obligaciones jurídicas, éticas y organizativas que no pueden ignorarse dependiendo del tipo de IA y del nivel de riesgo que implique. La responsabilidad no se limita al proveedor de la tecnología.

Y, como ocurrió con el RGPD en su momento, la llegada de la IA nos obligará a revisar procesos, introducir criterios nuevos de cumplimiento, reordenar contratos con proveedores y asegurarnos de que los equipos saben lo que pueden hacer y lo que no.

Lo que exige realmente el Reglamento de IA (RIA)

El RIA no consiste solo en controles técnicos o listas de requisitos. Su objetivo es que las organizaciones entiendan realmente qué están haciendo cuando usan IA. Y eso pasa por tres planos esenciales: identificar, valorar y supervisar.

A. Identificación. La IA puede llegar sin avisar: empleados que usan asistentes, traductores o generadores de texto sin consultarlo, aplicaciones que incorporan modelos avanzados sin decirlo, o herramientas gratuitas que parecen inocuas y no lo son. En estos escenarios —*shadow AI*— la organización puede estar enviando información interna, borradores de documentos que contengan información sensible, datos personales o contenido confidencial e incluso información protegida por secreto empresarial, a servicios de terceros países sin saberlo. Por esta razón se hace imprescindible que los equipos estén alfabetizados digitalmente en IA.

B. Valoración. Una vez detectado el uso, hay que entenderlo: qué hace, cómo lo hace, qué datos utiliza, qué licencias requiere para un uso comercial y qué consecuencias puede generar. Es aquí donde entran, en su caso, la realización de EIPD, FRIA, clasificación de usos de alto riesgo y la calidad de los datos. En esencia, se trata de definir qué herramientas pueden utilizarse y en qué condiciones.

C. Supervisión. Supervisar es mantener un control real —y demostrable— sobre el funcionamiento de la IA y esencialmente cuando los sistemas sean de riesgo alto. Implica poder explicar decisiones relevantes,

evitar usos fuera del marco previsto, garantizar que el personal sabe utilizar la herramienta sin comprometer datos o procesos y conservar registros suficientes para responder ante incidentes o auditorías.

La mayoría de los sistemas de IA funcionan con modelos opacos y flujos de datos poco visibles, lo que puede generar transferencias no detectadas, perfilado no previsto o fallos en la notificación de incidentes. Por ello, es clave documentar actividades críticas, monitorizar el sistema y contar con un protocolo rápido de respuesta ante incidentes.

El RGPD entra en escena (y entra con toda su fuerza)

Cada vez que una herramienta de IA procesa, infiere o genera resultados que afectan a personas identificables, el RGPD se activa por completo.

Licitud, información, minimización, límites al tipo de datos que se introducen y garantías frente a decisiones automatizadas: está todo ahí.

Muchas herramientas aparentan ser inocuas, pero generan procesos invisibles de perfilado, inferencia o tratamiento masivo. En estos casos, la obligación de realizar EIPDs puede convertirse en un requisito vinculante.

De nuevo aparece la importancia de los contratos: quién accede a los datos, si se usan para entrenar modelos, dónde se almacenan y qué pasa si el proveedor incumple.

El Data Act: el gran desconocido que también aplica

El Data Act impone obligaciones sobre el uso de datos generados por productos conectados o por terceros.

Cuando una organización alimenta una IA con datos que no le pertenecen, que no tiene derecho a reutilizar o que provienen de servicios conectados sujetos a restricciones, puede incurrir en infracciones contractuales, vulneraciones de secreto empresarial o accesos no autorizados.

El riesgo no nace solo del dato en sí, sino del uso que la IA hace de él, y de la trazabilidad que la organización es capaz —o incapaz— de acreditar.

Un régimen sancionador acumulativo y severo

El uso de IA no solo implica obligaciones, sino también un panorama sancionador transversal. El Reglamento de IA contempla sanciones por despliegue negligente, uso indebido, falta de supervisión o el empleo de sistemas prohibidos. Al mismo tiempo, el RGPD puede imponer multas de hasta el 4 % del volumen global de negocio cuando se vulneran derechos de protección de datos. El Data Act añade responsabilidad por usos indebidos o no autorizados de datos, y, en sectores regulados, pueden sumarse sanciones adicionales, restricciones operativas e incluso la suspensión de la actividad.

En conjunto, los riesgos se acumulan y subrayan la necesidad de que la organización realice una adecuación en materia de IA: revisar procesos, actualizar políticas y contratos, formar a los equipos y establecer controles que garanticen un cumplimiento riguroso y constante.

Contacto



Luis Marimón

Socio | Tecnología, Protección de Datos e IA

lmарimon@marimon-abogados.com

Barcelona

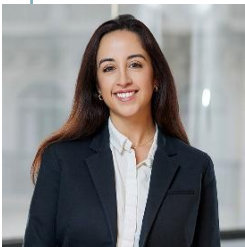


Maria Santa

Abogada | Tecnología, Protección de Datos e IA

msanta@marimon-abogados.com

Madrid

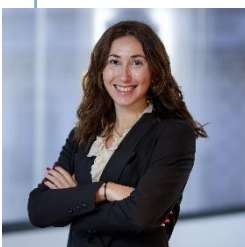


Laura Morató

Abogada | Tecnología, Protección de Datos e IA

lmorato@marimon-abogados.com

Barcelona



Laura Espinós

Abogada | Tecnología, Protección de Datos e IA

lespinos@marimon-abogados.com

Barcelona