IA EN LA EMPRESA: LOS RIESGOS LEGALES QUE DEBE CONOCER



Posted on 22. mayo 2026 by Tomás

Hoy en día, las empresas utilizan la IA para crear contenido, atender a sus clientes, lanzar campañas de marketing, analizar datos, seleccionar personal o automatizar procesos internos. Lo que hace unos pocos años parecía experimental **forma parte ya del día a día de muchas organizaciones.** Y ahí reside un riesgo creciente: el uso de la IA en la empresa avanza a un ritmo vertiginoso, mientras muchas compañías aún no han adaptado sus procesos internos, sus estándares de seguridad ni su cumplimiento normativo.

Lo más delicado es que la IA se utiliza a menudo de forma espontánea y sin reglas claras. Los empleados copian información confidencial en chatbots, los departamentos de marketing publican textos generados por IA sin revisarlos y las empresas confían en contenidos automatizados cuyo origen o exactitud apenas pueden comprobarse. Al mismo tiempo, aparecen nuevos requisitos legales, como el AI Act europeo (la ley de IA de la UE), que le obligan a actuar con mayor diligencia.

LOS 5 PRINCIPALES RIESGOS LEGALES DE LA IA EN LA EMPRESA

Si quiere utilizar la IA en su empresa, no basta con conocer sus oportunidades: **también debe entender los riesgos legales**. Estos son los cinco ámbitos de riesgo más importantes:

Ámbito de riesgo	Qué puede ocurrir en concreto

Protección de datos	Infracciones del RGPD al introducir datos personales en herramientas de IA externas
Propiedad intelectual	Derechos poco claros sobre los resultados de la IA; vulneración de derechos sobre obras ajenas por similitud
Alucinaciones	Responsabilidad por afirmaciones falsas publicadas, fuentes inventadas o datos de producto erróneos
Discriminación	Perjuicio a grupos de candidatos por datos de entrenamiento sesgados (Ley 15/2022 de igualdad de trato)
Regulación	Obligaciones del AI Act: documentación, transparencia, formación y gestión de riesgos

POR QUÉ LA IA SE HA CONVERTIDO DE REPENTE EN UN TEMA DE CUMPLIMIENTO NORMATIVO

Muchas empresas ven la IA sobre todo **como una herramienta de productividad**. Los textos se crean más rápido, los procesos se automatizan y las tareas repetitivas se resuelven con más eficiencia. Sin embargo, es precisamente esa rapidez la que hace que los riesgos pasen a menudo desapercibidos.

A diferencia del software tradicional, la IA genera contenidos y toma decisiones de forma autónoma. Puede cometer errores, ofrecer información incorrecta o producir contenidos problemáticos sin que se note a primera vista. La situación se vuelve crítica, sobre todo, cuando usted da por buenos y publica esos resultados sin revisarlos.

A esto se suma que muchos sistemas de IA trabajan con grandes volúmenes de datos. Si en ellos se procesan datos personales, documentos internos o información confidencial de clientes, los problemas de protección de datos y de responsabilidad no tardan en aparecer. Para usted, esto significa que la IA ya no es solo una cuestión técnica, sino cada vez más **una cuestión de cumplimiento normativo, gestión de riesgos y responsabilidad empresarial.**

PROTECCIÓN DE DATOS: LA PRINCIPAL PUERTA DE ENTRADA

En la práctica, la mayoría de los problemas surgen actualmente en el manejo de datos sensibles. Muchos empleados usan las herramientas de IA como si fueran un buscador e introducen

información sin pensar en las consecuencias. Y eso puede salir caro.

Salvo que disponga de una licencia empresarial (versión Enterprise) con garantías claras de protección de datos, los siguientes datos no deberían introducirse nunca en herramientas de IA públicas como ChatGPT, Gemini o Claude:

- Datos de clientes (nombres, datos de contacto, historial de pedidos)
- Candidaturas y currículums
- Contratos, presupuestos y cálculos internos de precios
- Datos de empleados y de salud
- Credenciales de acceso, claves API y contraseñas
- Documentos internos de estrategia y finanzas

Según la plataforma, los contenidos introducidos pueden almacenarse, analizarse o utilizarse para mejorar los modelos. Desde el punto de vista del RGPD, esto es relevante porque los datos personales solo pueden tratarse en condiciones claramente definidas. **Si faltan directrices internas o medidas técnicas de protección, surgen riesgos legales** que pueden derivar en sanciones y en la obligación de notificar la brecha a la autoridad de control (en España, la AEPD).

También se subestima lo descontrolado que es ya el uso interno de la IA. A menudo no existen procesos de aprobación ni normas sobre qué herramientas pueden utilizarse. Así aparece el llamado fenómeno de la «Shadow AI» (IA en la sombra): los empleados trabajan por su cuenta con aplicaciones de IA sin que la dirección sepa qué datos se están procesando en ellas.

CONTENIDOS GENERADOS POR IA Y EL PROBLEMA DE LA PROPIEDAD INTELECTUAL

Otro gran riesgo afecta a la propiedad intelectual. Muchas empresas dan por hecho que los textos, imágenes o diseños generados por IA les pertenecen automáticamente. La situación jurídica no es tan sencilla.

En España, la Ley de Propiedad Intelectual considera autor a la persona natural que crea la obra (art. 5) y protege **las creaciones originales** (art. 10). Por eso, los contenidos generados exclusivamente por IA, sin una aportación creativa humana relevante, difícilmente están protegidos por derechos de autor. Lo que cuenta es el peso real de la aportación creativa propia. Para departamentos de marketing, agencias y productores de contenido, esto es muy relevante: en principio, terceros podrían reutilizar libremente contenidos creados únicamente por IA.

Al mismo tiempo existe el riesgo contrario: la IA puede copiar o imitar obras existentes sin querer. Sobre todo en imágenes, diseños, logotipos o campañas creativas pueden aparecer similitudes con ellas. En ese caso, usted corre el riesgo de vulnerar derechos de autor o de marca de terceros, lo que puede acarrear reclamaciones e indemnizaciones.

Además, existe un problema práctico: los sistemas de IA generan contenidos a partir de enormes volúmenes de datos de entrenamiento. El origen de estilos, formulaciones o elementos visuales concretos **apenas puede rastrearse**. Quien publica resultados de la IA sin revisarlos se mueve, por tanto, en una **zona gris legal.**

EL RIESGO SUBESTIMADO DE LAS ALUCINACIONES

Uno de los mayores problemas de los sistemas de IA actuales es su capacidad para generar información falsa de forma convincente. Son las llamadas alucinaciones: suelen parecer creíbles y estar redactadas de forma profesional, **aunque su contenido sea incorrecto.**

En marketing y contenidos, esto supone un riesgo considerable. La IA puede generar datos de producto erróneos, inventar estudios, citar fuentes de forma incorrecta o formular afirmaciones técnicas que sencillamente no son ciertas. Para los lectores, a menudo no es evidente que el contenido proceda de una IA, **pero el responsable sigue siendo usted**.

Si comunica promesas falsas sobre sus productos o servicios o difunde información engañosa, puede incurrir en actos de engaño tipificados en la Ley de Competencia Desleal, con reclamaciones, indemnizaciones y daños a la reputación. En ámbitos sensibles como la salud, las finanzas o el derecho, esto puede llegar a poner en peligro la supervivencia de la empresa.

Por eso no basta con leer los textos de IA por encima. Necesita **controles de calidad claros** y una **aprobación humana obligatoria** antes de que cualquier contenido salga de la empresa.

LA SELECCIÓN DE PERSONAL Y LAS DECISIONES AUTOMATIZADAS CONLLEVAN NUEVOS RIESGOS

Cada vez más empresas recurren también a la IA en la selección de personal. Las candidaturas se analizan de forma automatizada, los currículums se preclasifican y los candidatos se evalúan según determinados criterios. Y es aquí donde aparecen riesgos de discriminación considerables.

Los sistemas de IA aprenden de datos existentes. Si esos datos están sesgados o contienen prejuicios inconscientes, **la IA reproduce esos patrones**. Así, determinados grupos de personas salen perjudicados sin que se note de inmediato. Esto choca frontalmente con la Ley 15/2022, integral para la igualdad de trato y la no discriminación.

Para su empresa, las **consecuencias pueden ser graves**: acusaciones de discriminación, daños de imagen, conflictos legales y reclamaciones de indemnización de candidatos rechazados. La situación es especialmente crítica cuando las decisiones se toman de forma totalmente automatizada y ya no existe ningún control humano. Por eso, el AI Act clasifica los sistemas de IA para recursos humanos como aplicaciones de alto riesgo.



EL AI ACT DE LA UE CAMBIA LAS REGLAS DEL JUEGO

El AI Act es **el primer marco legal integral para la inteligencia artificial en Europa**. El reglamento entró en vigor el 1 de agosto de 2024 y se aplica de forma escalonada. En España, la supervisión de los sistemas de IA corresponde a la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Muchas empresas siguen subestimando el impacto concreto que tendrá esta ley de IA en los próximos meses.

El AI Act sigue un enfoque basado en el riesgo: cuanto mayor es el riesgo potencial de un sistema de IA, más estrictos son los requisitos. Se prevén cuatro niveles de riesgo:

Nivel de riesgo	Ejemplos	Consecuencias para usted
Inaceptable	Puntuación social, sistemas manipuladores, reconocimiento de emociones en el lugar de trabajo	Prohibidos desde febrero de 2025
Alto riesgo	IA para selección de personal, evaluación de solvencia, identificación biométrica, infraestructuras críticas	Obligaciones estrictas: gestión de riesgos, documentación, supervisión humana
Riesgo limitado	Chatbots, deepfakes, contenidos generados por IA	Obligación de transparencia: el usuario debe poder reconocer que interviene una IA
Riesgo mínimo	Filtros de spam, IA en videojuegos	Sin obligaciones especiales

Las obligaciones se aplican de forma escalonada. Para su planificación, es importante tener en cuenta:

- Desde febrero de 2025: prohibición de determinadas prácticas de IA y alfabetización en IA obligatoria (AI Literacy) para los empleados que utilizan IA
- Desde agosto de 2025: obligaciones para los proveedores de modelos de IA de uso general (como GPT, Claude o Gemini)
- Desde agosto de 2026: la mayoría de las obligaciones para sistemas de alto riesgo y para los responsables del despliegue (las empresas que utilizan IA) pasan a ser plenamente aplicables
- A partir de agosto de 2027: finalizan los periodos de transición para la IA de alto riesgo integrada en productos regulados

Importante: la obligación de alfabetización en IA (art. 4 del AI Act) **ya está en vigor y afecta prácticamente a cualquier empresa que utilice IA**. Si no puede acreditar que ha formado a su plantilla en el uso responsable de la IA, ya está incumpliendo el reglamento.

POR QUÉ NECESITA YA REGLAS CLARAS PARA LA IA EN SU EMPRESA

Actualmente, el mayor peligro no suele estar en la tecnología en sí, sino en la falta de gobernanza dentro de las empresas. Muchas organizaciones toleran tácitamente el uso de la IA sin haber definido procesos ni responsabilidades claras. Esto plantea una serie de preguntas sin resolver:

- ¿Quién puede utilizar qué herramientas?
- ¿Qué datos pueden introducirse y cuáles no?
- ¿Cómo se revisan los contenidos de IA antes de publicarlos?
- ¿Quién asume la responsabilidad en caso de errores o infracciones?
- ¿Cómo se documenta el uso de la IA?

Una política de IA eficaz cubre, como mínimo, los siguientes ámbitos:

- **Aprobación de herramientas:** lista de las herramientas de IA autorizadas y de sus ámbitos de uso
- **Clasificación de datos:** reglas claras sobre qué tipos de datos pueden tratarse en qué herramientas
- **Proceso de aprobación:** revisión humana obligatoria antes de publicar contenidos generados por IA
- **Formación:** cursos documentados de alfabetización en IA para todos los empleados con acceso a herramientas de IA
- **Etiquetado de contenidos de IA:** reglas de transparencia para la comunicación externa

generada por IA

- **Gestión de incidentes:** canales de notificación y responsables ante incidentes de protección de datos o de cumplimiento

Lo esencial es esto: la IA no sustituye la responsabilidad humana. Usted sigue siendo responsable de los contenidos publicados, de las decisiones y del tratamiento de datos, independientemente de que los haya generado una persona o una máquina.

CONCLUSIÓN: LA IA EN LA EMPRESA OFRECE UN ENORME POTENCIAL, PERO NO ES UN ATAJO LEGAL

La inteligencia artificial transformará a fondo el mundo laboral. Le permite acelerar procesos, reducir costes y crear nuevas oportunidades. Al mismo tiempo, plantea retos legales que muchas empresas todavía subestiman.

La protección de datos, la propiedad intelectual, la responsabilidad, la discriminación y los requisitos regulatorios ganarán mucho peso en los próximos años. El camino más peligroso es el uso descontrolado, sin reglas ni responsables.

Si quiere utilizar la IA con éxito a largo plazo, necesita algo más que buenas herramientas. La clave está en unos procesos claros, empleados formados, medidas técnicas de seguridad y un uso responsable de la tecnología.

La IA puede acelerarlo casi todo, también los problemas legales.

En **Wisea** ayudamos a las empresas a integrar los procesos de IA en su marketing de forma estructurada y práctica. Apostamos por el control humano, estándares de calidad claros y un manejo responsable de los datos y contenidos sensibles.

Los buenos resultados no nacen de una automatización descontrolada, sino de la combinación inteligente de tecnología, conocimiento especializado y experiencia. ¿Quiere introducir la IA en su empresa de forma segura? No dude en ponerse en contacto con nuestra agencia.