



Checklist práctica AI Act 2026

Guía operativa para empresas y organizaciones

Esta guía es una versión orientativa, basada en el Reglamento (UE) 2024/1689 (AI Act). Su propósito es ofrecer a empresas y organizaciones una referencia práctica para iniciar o fortalecer el cumplimiento normativo de sus sistemas de IA.

El AI Act establece un marco regulador común en la Unión Europea, centrado en la seguridad, los derechos fundamentales y la confianza en el desarrollo y uso de sistemas de inteligencia artificial.

“ La inteligencia artificial dejó de ser simplemente una herramienta: hoy es una decisión regulada.”

El cumplimiento no comienza cuando aparece una obligación, sino cuando la organización decide anticiparse. Esta checklist está diseñada para ayudarte a revisar los aspectos clave antes de que el crecimiento convierta pequeños descuidos en problemas mayores.

Consulta el texto oficial del AI Act en [EUR-Lex](#) y la [Estrategia Digital Europea](#) para comprender el contexto más amplio de la regulación y su relación con la innovación responsable.

Esta guía no sustituye el asesoramiento legal, pero puede ser el primer paso hacia una cultura de cumplimiento sólida, proactiva y sostenible.



Primero, una realidad incómoda: «soy pequeño» no es una estrategia de cumplimiento

El Reglamento (UE) 2024/1689 —conocido como Ley de IA— introduce un enfoque basado en el riesgo, no en el tamaño de la empresa.

Es decir: si tu sistema de IA es de alto riesgo, las obligaciones son las mismas tengas dos personas en plantilla o dos mil.

Las multas lo dejan claro: hasta **35 millones de euros o 7 %** del volumen de negocios anual mundial total, si se infringen las prohibiciones o los requisitos en materia de prácticas de IA de alto riesgo; hasta 15 millones de euros o 3 % en los demás casos.

Sí, has leído bien. Por proporcionalidad, si la Unión Europea prevé alcantarías estas sanciones atendiendo al tamaño y capacidad económica del infractor. En la práctica, para pymes, startups y pequeñas empresas de mediana capitalización, las cantidades efectivas serán menores que los techos máximos.

Pero el cumplimiento no es opcional. Y adoptar un enfoque proporcional no significa aplazar decisiones.

La buena noticia es que, con un marco claro y proporcional a tu realidad, empezar a ordenar tu negocio puede ser mucho más sencillo de lo que imaginas.



¿Dónde y para qué estoy utilizando inteligencia artificial?



Tu Checklist AI Act: empieza por estos 8 controles

Ocho controles prácticos para pymes que quieren usar IA con seguridad, cumplir el EU AI Act y proteger su negocio sin frenar la innovación.



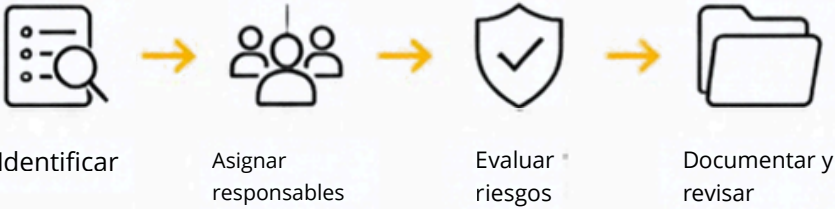
1. INVENTARIO DE SISTEMAS DE IA

Saber qué IA usamos es el primer paso para gestionarla.

Ejemplos de herramientas de IA:

- ChatGPT / GPTS personalizados
- Microsoft 365 Copilot
- Google Gemini
- Claude (Anthropic)
- Midjourney / DALL E
- Notion AI
- Perplexity AI
- Fireflies.ai
- Otras internas o a medida

Mini esquema visual (inventario)



Herramienta	Para qué la utilizamos	Quién la utiliza	Qué datos recibe

2. CLASIFICACIÓN DEL RIESGO

No todas las IA son iguales. El AI Act clasifica los sistemas según el riesgo que pueden suponer para las personas.

No preguntes solamente qué herramienta utilizas. Pregunta qué hace por ti.

Para garantizar un uso adecuado de la IA en nuestra empresa, clasificamos las aplicaciones según el impacto que tienen en nuestros procesos, en otras personas y en nuestros clientes.

Esta matriz de cuatro niveles permite identificar el tipo de autorización, el nivel de revisión y los riesgos asociados a cada uso.

1. Usa interno o de apoyo

Herramientas que apoyan actividades internas sin impacto directo en terceros.

Ejemplos: asistentes de redacción, organizadores de tareas, generadores de ideas, análisis de documentos internos.

Riesgos: Fuga de información interna, uso indebido de datos corporativos.

Controles requeridos: Uso permitido con formación básica en privacidad y buenas prácticas.

2. Interacción o comunicación externa

Herramientas que interactúen con clientes, proveedores o el público.

Ejemplos: chatbots, asistentes, contenidos, comunicaciones automatizadas

Controles requeridos: revisión periódica de los documentos de contratación y contratos, trazabilidad de interacciones. Anunciar cuando interviene una IA en lugar de una persona.

3. Decisiones o evaluaciones sobre personas:

Ejemplos: contratación, scoring, selección, determinados perfiles o biometría.

Riesgos: Información incorrecta, falta de criterio, gestión inadecuada de la empresa. Discusiones o evaluaciones dudosas sobre personas.

Controles requeridos: El factor humano siempre debe estar presente y se debe garantizar la protección de los datos de las personas.

4. Posibles prácticas prohibidas o usos especialmente sensibles:

Aquí debes detenerte y comprobar el caso concreto antes de continuar.

La UE prohíbe determinados usos de IA, entre ellos ciertas técnicas manipuladoras o engañosas que causen o puedan causar perjuicios significativos, determinadas formas de explotación de vulnerabilidades, social scoring, ciertos usos de policía predictiva, determinadas formas de categorización biométrica y el reconocimiento de emociones en lugares de trabajo o centros educativos salvo excepciones concretas.

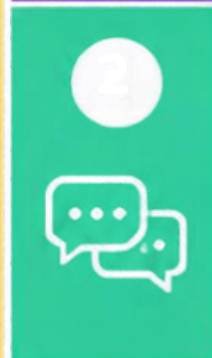
Controles requeridos: prohibición expresa. Evaluación ética y legal previa a su desarrollo o implementación.

MATRIZ DE LOS 4 NIVELES DE USO DE IA



USO INTERNO O APOYO

- Apoya actividades internas
- sin impacto directo en terceros.
- Ejemplos: asistentes de redacción, organizadores de tareas, generadores de ideas, diseñadores internos.
- Riesgos: fuga de información interna, base de de datos corporativos.
- Controles requeridos:



INTERACCIÓN O COMUNICACIÓN EXTERNA

Interactuar con clientes, proveedores

- Ejemplos: chats, generadores de contenido, evaluadores de servicio.
- Riesgos: información incorrecta, falta de transparencia, presentación inadecuada de la empresa.



DECISIONES O EVALUACIONES SOBRES PERSONAS

- Analiza o toma decisiones que afectan derechos, oportunidades o condiciones de personas.
- Ejemplos: filtrado de candidatos, detección de fraudes, evaluaciones de desempeño.
- Riesgos: decisiones autónomas del algoritmo, sesgos ocultos, opacidad en decisiones.



POSIBLES PRÁCTICAS PROHIBIDAS O ESPECIALMENTE SENSIBLES

- Pueden violar derechos fundamentales, leyes o principios típicos esenciales.
- Ejemplos: violación de emoción, perfiles sin consentimiento, decisiones automáticas sin supervisión.
- Riesgos: violaciones legales graves, daños reputacionales, sanciones regulatorias.

CONTROL 3:

Comprueba si tus clientes están hablando con una IA

El artículo 50 establece que, cuando un sistema de IA genere contenido, se deberá informar de ello a la persona física que esté expuesta al mismo de forma clara y visible.

La Comisión pondrá a disposición formatos actualizados para esta información, con el fin de asegurar una aplicación coherente en toda la UE en el marco de la Estrategia Digital Europea.

Las obligaciones dependen del tipo de contenido y de quién sea proveedor o responsable del despliegue.

CANALES DEL CONTROL 3:

	Web Información clara y destacada en la página o sección donde se genere el contenido.
	Chat Aviso visible al inicio de la conversación y recordatorios periódicos.
	Atención automatizada Aviso al inicio y durante la interacción automatizada (voz o texto).
	Asistentes o agentes Identificación clara y persistente de que se trata de un sistema de IA.
	Otros canales digitales Adaptar el aviso al formato y contexto específicos de cada canal digital utilizado.

EJEMPLOS:



"Hola, soy Laura. ¿En qué puedo ayudarte?"



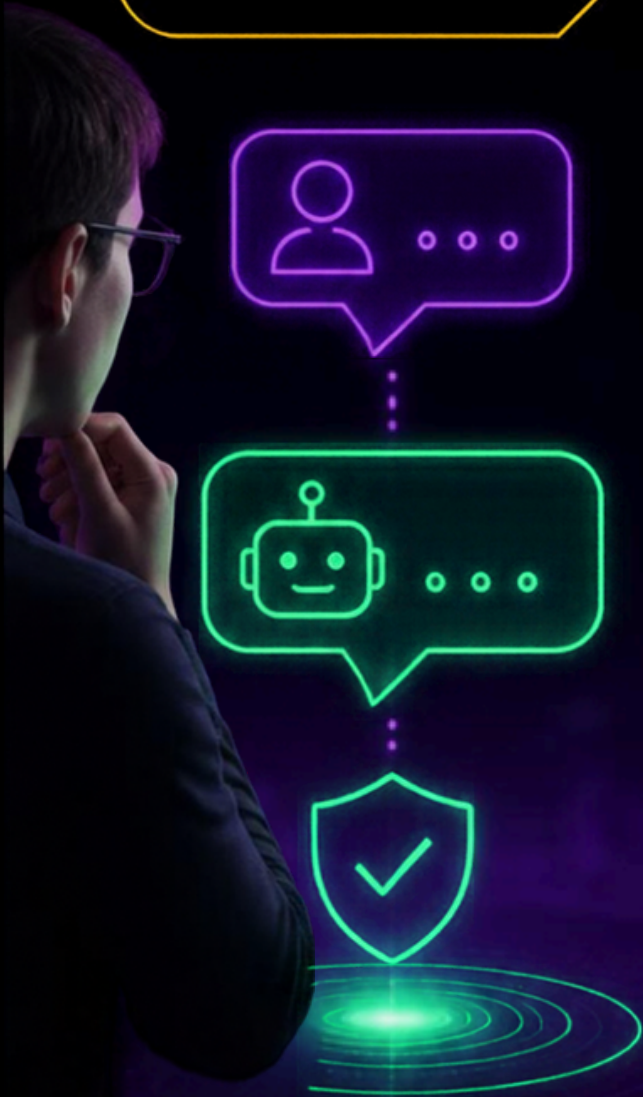
"Hola. Soy el asistente virtual de IA de [Marca]. Puedo ayudarte con..."



Transparencia desde la primera interacción

Informar de forma clara, visible y oportuna no es solo una obligación legal: es la base de la confianza.

Una comunicación honesta desde el inicio mejora la experiencia y fortalece la relación con las personas.



CONTROL 4:

CREA TU CHECKLIST DE CONTENIDO DE IA

Para los negocios que utilizan IA, uno de los casos especialmente relevantes son los **deepfakes** o contenidos sintéticos que simulan de forma realista a personas diciendo o haciendo algo que nunca ocurrió. Estos pueden dañar reputaciones, engañar a clientes o empleados, y generar consecuencias legales serias.

Por eso, el **article 50 del AI Act** prohíbe expresamente su uso cuando causen daño.

Además, la **Estrategia Digital Europea 2030** refuerza la necesidad de entornos digitales seguros, confiables y centrados en las personas.

Antes de publicar cualquier contenido generado o alterado con IA, pregúntate:



- ☐ ¿Este contenido incluye elementos **generados o alterados por IA**?
- ☐ ¿Contiene **representación** de personas, voces o situaciones que podrían parecer reales?
- ☐ ¿Tiene este contenido potencial para **engañar** o causar **daño**?
- ☐ ¿Ha sido **revisado por una persona** antes de su publicación?
- ☐ ¿Se **divulgará de forma visible o audible** que el contenido ha sido generado o alterado con IA?

CONTROL 5:

NO TE VAYAS A LOS EXTREMOS

No necesitas convertir a todo tu equipo en ingenieros de **machine learning**.

Este es probablemente uno de los puntos que más pequeños negocios han pasado por alto.

Según el **artículo 4 del AI Act**, desde el **2 de febrero de 2025**, tienes que enseñar a tu equipo a usar IA de forma competente según su rol.

Además, la **Estrategia Digital Europea 2030** refuerza este principio para construir una Europa digital donde nadie quede atrás.

Necesitas conseguir que las personas que utilizan IA comprendan lo suficiente para hacerlo responsablemente según su función y contexto.



- ☐ Qué **herramientas** están autorizadas.
- ☐ Para qué puede utilizarse cada una.
- ☐ Qué **información** no debe introducirse indiscriminadamente.
- ☐ Cómo detectar **errores** y **alucinaciones**.
- ☐ Cuándo **revisar manualmente** un resultado.
- ☐ Qué usos requieren transparencia.
- ☐ Cuándo **detener** una automatización y **escalar** la decisión a una persona.
- ☐ Qué usos están **prohibidos** o requieren **análisis especializado**.

No enseñes únicamente prompts. Enseña criterio.



CONTROL 6.

Comprueba qué datos estás introduciendo en sistemas de IA

El **AI Act** no sustituye al **RGPD**.

Sigue siendo aplicable el Reglamento General de Protección de Datos, y la **Agencia Española de Protección de Datos** sigue siendo la autoridad competente en esta materia.

Si los datos que usas pueden afectar a **derechos y libertades** de las personas, podrías necesitar hacer una **Evaluación de Impacto relativa a la Protección de Datos**.

Haz una lista de comprobación:

- ☐ ¿Introduce nombres de clientes?
- ☐ ¿Emails o teléfonos?
- ☐ ¿Conversaciones privadas?
- ☐ ¿CV o información de candidatos?
- ☐ ¿Bases de datos?
- ☐ ¿Documentos internos con información personal?
- ☐ ¿Información sensible o confidencial?
- ☐ ¿Imágenes, voces u otros datos identificables?

¿Realmente **necesito enviar** esos datos al sistema de IA para conseguir el resultado que busco?

Aplica el **principio de minimización**: introduce solo lo esencial o **anonimiza** los datos siempre que sea posible.

Consulta la guía práctica **Facilita RGPD** para más detalles sobre cómo proteger los datos personales. **¡No subas información personal a la nube sin saber dónde se guarda ni quién puede acceder a ella!**



□ **CONTROL 7. Define dónde termina la IA y empieza la decisión humana**

PAGE 9

No todas las decisiones pueden o deben automatizarse. Define y documenta qué puede hacer la IA (asistir, recomendar, resumir) y qué decisiones finales siempre requieren intervención humana.

¿Qué puede recomendar la IA y qué debe decidir una persona?

Ejemplo: la IA puede resumir diez currículums y recomendar los tres más alineados. La persona decide a quién entrevistar.

El AI Act pone el foco especialmente en decisiones que afectan a personas en contextos como:

- Contratación.
- Acceso a determinados servicios.
- Evaluación de personas.
- Scoring.
- Biometría.
- Decisiones con consecuencias relevantes para clientes, trabajadores o candidatos.



□ **CONTROL 8. Crea tu «Registro Básico de IA»**

Lleva un registro básico de las herramientas de IA que utilizas en tu organización. No sustituye a los registros formales que exige el AI Act para sistemas de alto riesgo, pero te ayuda a tener visibilidad y control. Te servirá para gestionar, revisar y demostrar cumplimiento.

- Puedes hacerlo en una simple hoja de cálculo donde incluyas:
 - Herramienta de IA
 - Proveedor
 - Finalidad
 - Área responsable
 - Personas que la utilizan
 - ¿Interactúa con clientes?
 - ¿Utiliza datos personales?
 - ¿Genera contenido externo?
 - ¿Interviene en decisiones sobre personas?
 - ¿Requiere aviso de transparencia?
 - ¿Tiene revisión humana?
 - Nivel de atención: bajo / revisar / especializado
 - Fecha de última revisión

TU PLAN DE ACCIÓN DE

7 DÍAS

Este registro te permitirá detectar algo que sucede constantemente en pequeños negocios:

- Una persona instala una herramienta.
- Otra conecta una automatización.
- Otra emplea a utilizar IA generativa.
- Seis meses después, nadie sabe realmente cuántos sistemas de IA forman parte del negocio.
- La gobernanza empieza por recuperar esa visibilidad.

1

DÍA 1: INVENTARIO

Detecta todas las herramientas que ya utilizas con IA.

2

DÍA 2: CLASIFICACIÓN

Determina el nivel de riesgo de cada herramienta: mínimo, limitado, alto o inaceptable.

3

DÍA 3: CHATBOTS Y PUNTOS DE CONTACTO

Configura avisos de uso de IA donde interactuas con personas.

4

DÍA 4: CREACIÓN Y PUBLICACIÓN DE CONTENIDO GENERADO O MANIPULADO

Añade avisos visibles en imágenes, audios, videos y textos.

5

DÍA 5: DATOS PERSONALES

Revisa qué datos recoges, para qué los usas y con qué herramientas.

6

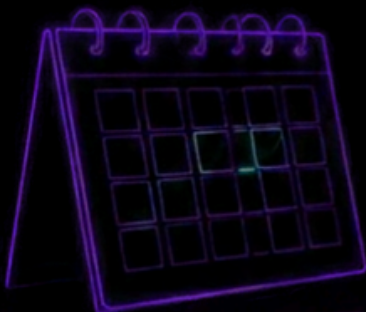
DÍA 6: POLÍTICA INTERNA Y FORMACIÓN

Documenta tu política de IA y forma a tu equipo en buenas prácticas.

7

DÍA 7: USOS SENSIBLES Y REVISIÓN ESPECIALIZADA

Evalúa usos de alto impacto o riesgo. Si tienes dudas, consulta con un experto.



Al terminar tendrás algo mucho más valioso que un documento: un sistema de confianza que protege tu negocio y mejora tu reputación.

TRANQUILIDAD:

CUMPLIR NO SIGNIFICA PARALIZAR TU NEGOCIO

Después de leer sobre obligaciones, transparencia, riesgos y sanciones, es fácil caer en el extremo contrario:

«ENTONCES MEJOR NO UTILIZO IA.»

No. El AI Act no quiere frenar la innovación; busca que la IA se use con seguridad, transparencia y respeto a los derechos. Su filosofía es simple: no prohíbe la IA, prohíbe los usos inaceptables y te pone responsabilidad cuando puede haber riesgos.

Funciona con un **enfoque basado en riesgos**: cuanto mayor sea el impacto potencial en las personas, más obligaciones y controles debes aplicar.

Por eso, empieza poco a poco y progresa paso a paso. Puedes usar esta secuencia como **hoja de ruta**:



Cómo empezar hoy:

- ✓ Crea un inventario simple (por ejemplo, una **hoja de cálculo**) de las IA que usas.
- ✓ Redacta una **política interna clara** sobre usos permitidos y prohibidos.
- ✓ Forma a tu equipo con **formación básica** en riesgos y buen uso.
- ✓ Define **controles editoriales** antes de publicar o decidir con IA.
- ✓ Revisa de forma **profesional** cuando el impacto pueda afectar a personas.



IMPORTANTE: ESTA CHECKLIST NO PUEDE DECIRTE POR SÍ SOLA TODO LO QUE DEBES CUMPLIR

Solo sirve para ayudarte a **orientarte**. Cada caso tiene matices que dependen del contexto, la tecnología usada, los datos tratados y quién se ve afectado.

Ejemplos:

- Una **agencia** que usa IA para generar imágenes promocionales.
- Una empresa que usa un **chatbot** para atención al cliente.
- Un **ecommerce** que recomienda productos según el comportamiento de compra.
- Un sistema que apoya la **selección de trabajadores**.
- O una **solución que analiza datos biométricos, de salud o información especialmente sensible**.

En todos estos casos pueden aplicarse obligaciones distintas según el riesgo, incluidos los sistemas de **alto riesgo**.

Además, algunas disposiciones del AI Act tienen **calendarios específicos** y las obligaciones pueden coexistir con otras normas, entre ellas el **RGPD**.

Por eso esta checklist representa un **punto de partida operativo**, no una certificación de cumplimiento ni tampoco pretende sustituir una asesoría legal.

DESCUBRIMOS DÓNDE SE NECESITA CLARIDAD.

Te ayudamos a traducir el AI Act a tu contexto, sin burocracia innecesaria.



¿Quieres aterrizarlo específicamente a tu negocio?

☐

¿Cómo debería **comunicar** que utilizo IA?

☐

¿Qué tenemos que **modificar** en nuestros contenidos?

☐

¿Cómo integramos **transparencia** sin destruir la experiencia del cliente?

☐

¿Qué **procesos** de marketing deberíamos revisar?

☐

¿Cómo **aterrizamos** todo esto en nuestra web, contenidos, automatizaciones y comunicación?



Antes de cerrar:
una aclaración importante sobre nuestro trabajo

En [The Invictus Lab](#) puedes consultar nuestro servicio de [consultas personalizadas 1:1](#) para profundizar, resolver dudas concretas y adaptar estas recomendaciones a tu caso real.

Nunca tendrás respuestas genéricas, sino orientación experta pensada para tu realidad.