

Checklist de alfabetización en IA

Artículo 4

RECURSO DE TRABAJO

Un recorrido operativo para identificar a quién formar, adaptar los contenidos al contexto, dejar evidencia y mantener las medidas vivas. No es un certificado ni sustituye asesoramiento jurídico.

ANTES DE EMPEZAR

Qué debe resolver el programa

El artículo 4 no define un curso único ni un número fijo de horas. Las medidas deben responder a las personas, los sistemas, el riesgo y el contexto real de uso.

01

Personas

Personal y terceros que operan o usan sistemas de IA por cuenta de la organización.

02

Contexto

Conocimientos previos, experiencia, sector, finalidad y personas potencialmente afectadas.

03

Sistemas

Qué IA se usa, quién la proporciona, para qué decisiones y con qué datos.

04

Medidas

Formación, guías, controles, práctica, soporte y seguimiento adecuados a cada rol.

ACTUALIZACIÓN REGULATORIA · 27 JUL 2026

El artículo 4 vigente exige medidas adaptadas y documentables.

El Reglamento (UE) 2026/1744 se publicó el 24 de julio y entró en vigor el 27 de julio de 2026. El artículo 4 exige adoptar medidas para apoyar la promoción de la alfabetización en IA, adaptadas al conocimiento, la experiencia, la educación, la formación y el contexto de las personas y grupos afectados. No exige garantizar un nivel específico en una persona concreta.

Cómo usar este documento

- 1 Marca Sí, Parcial, No o N/A y añade una referencia a la evidencia.
- 2 Convierte cada No o Parcial en una acción con responsable y fecha.
- 3 Escala los usos de alto impacto, las prácticas potencialmente prohibidas y las dudas de privacidad o seguridad.
- 4 Revisa el programa cuando cambien las herramientas, el riesgo, los roles o las instrucciones internas.

01 · DIAGNÓSTICO

Mapa de uso y responsabilidades

La alfabetización empieza por saber dónde está la IA y quién decide sobre su uso.

MARCA UNA OPCIÓN POR CONTROL

☐ SÍ ☐ PARCIAL ☐ NO ☐ N/A

01	Existe un inventario actualizado de sistemas y herramientas de IA, incluidas las adquiridas dentro de otras aplicaciones.	☐	☐	☐	☐
02	Cada uso tiene finalidad de negocio, responsable y personas usuarias identificadas.	☐	☐	☐	☐
03	Se distingue si la organización actúa como proveedor, responsable del despliegue o ambas cosas.	☐	☐	☐	☐
04	Se han identificado personal, colaboradores y terceros que operan o usan IA por cuenta de la organización.	☐	☐	☐	☐
05	Se documentan conocimientos previos, experiencia, funciones y exposición al riesgo de cada colectivo.	☐	☐	☐	☐
06	Se conoce qué datos entran, qué resultados salen y dónde se incorporan a procesos o decisiones.	☐	☐	☐	☐
07	Se han identificado personas o grupos potencialmente afectados por cada uso.	☐	☐	☐	☐
08	Existe un área o persona de referencia para dudas, autorizaciones e incidentes relacionados con IA.	☐	☐	☐	☐
09	Hay un catálogo de herramientas permitidas, restringidas y no autorizadas.	☐	☐	☐	☐
10	Existe un procedimiento para solicitar y evaluar una herramienta o uso nuevo antes de utilizarlo.	☐	☐	☐	☐
● Regla operativa: una herramienta no validada no debe utilizarse con información o para procesos de la empresa.					

Alfabetización general y por rol

Un bloque común crea lenguaje compartido; los módulos por rol conectan ese conocimiento con el trabajo real.

MARCA UNA OPCIÓN POR CONTROL

☐ SÍ ☐ PARCIAL ☐ NO ☐ N/A

01	El bloque común explica qué es la IA, cómo aprende, qué puede hacer y qué no puede garantizar.	☐	☐	☐	☐
02	Se explica la IA generativa: prompts, contexto, generación probabilística y límites de los resultados.	☐	☐	☐	☐
03	La formación incorpora los sistemas y casos de uso reales autorizados en la organización.	☐	☐	☐	☐
04	Se diferencian contenidos para usuarios generales, responsables, perfiles técnicos y funciones de control.	☐	☐	☐	☐
05	El nivel y la profundidad se adaptan a conocimientos, experiencia, educación y formación previos.	☐	☐	☐	☐
06	Se aborda el papel de la organización y las responsabilidades asociadas a proveedor y responsable del despliegue.	☐	☐	☐	☐
07	Se explican las categorías relevantes del AI Act: prácticas prohibidas, alto riesgo y transparencia.	☐	☐	☐	☐
08	Los colectivos que supervisan decisiones reciben formación específica sobre límites, escalado y autoridad para detener.	☐	☐	☐	☐
09	El personal conoce las políticas, protocolos y canales internos aplicables a su función.	☐	☐	☐	☐
10	Terceros que usan IA por cuenta de la empresa reciben medidas adecuadas o aportan evidencia suficiente.	☐	☐	☐	☐
● No hace falta que todas las personas sepan lo mismo. Sí hace falta que cada una sepa operar con criterio en su contexto.					

03 · CONTENIDOS

Riesgos, reglas y práctica

El conocimiento mínimo debe poder aplicarse antes, durante y después de usar la herramienta.

MARCA UNA OPCIÓN POR CONTROL

☐ SÍ☐ PARCIAL☐ NO☐ N/A

01	Se practican alucinaciones, errores y técnicas de verificación con fuentes independientes.	☐	☐	☐	☐
02	Se explican sesgos, discriminación, accesibilidad y efectos distintos sobre grupos de personas.	☐	☐	☐	☐
03	Se indican datos personales, sensibles, confidenciales o secretos que no deben introducirse sin autorización.	☐	☐	☐	☐
04	Se cubren propiedad intelectual, licencias, secretos empresariales y revisión de materiales generados.	☐	☐	☐	☐
05	Se enseña prompting seguro: objetivo, límites, datos mínimos, formato de salida y criterios de calidad.	☐	☐	☐	☐
06	Se definen tareas que requieren revisión humana y quién tiene autoridad para aprobar, corregir o detener.	☐	☐	☐	☐
07	Se explica cuándo informar de que se interactúa con IA o de que un contenido ha sido generado o manipulado.	☐	☐	☐	☐
08	Se reconocen ataques y fallos relevantes: prompt injection, fuga de información y resultados manipulados.	☐	☐	☐	☐
09	Se usan casos del sector con consecuencias realistas, no solo ejemplos genéricos.	☐	☐	☐	☐
10	Hay ejercicios y evaluación que comprueban decisiones seguras, además de recordar conceptos.	☐	☐	☐	☐

● Una respuesta fluida no es una respuesta cierta. La verificación y la supervisión forman parte del uso, no son un paso opcional.

04 · IMPLANTACIÓN

Evidencias y continuidad

El objetivo no es acumular certificados, sino poder explicar qué medidas se tomaron, para quién y por qué eran adecuadas.

MARCA UNA OPCIÓN POR CONTROL

☐ SÍ ☐ PARCIAL ☐ NO ☐ N/A

01	Existe un plan aprobado con objetivo, alcance, colectivos, contenidos, modalidad y responsables.	☐	☐	☐	☐
02	Se conserva la versión del temario, materiales, protocolos e instrucciones entregadas.	☐	☐	☐	☐
03	Se registran convocatorias, asistencia o finalización y fecha de la medida.	☐	☐	☐	☐
04	Se conserva evidencia de ejercicios, evaluación, incidencias de aprendizaje y acciones de refuerzo.	☐	☐	☐	☐
05	Los registros relacionan la medida con roles, herramientas o contextos de uso concretos.	☐	☐	☐	☐
06	El alta de nuevos usuarios incorpora orientación antes de acceder a herramientas relevantes.	☐	☐	☐	☐
07	Hay recordatorios o refuerzos cuando cambian herramientas, riesgos, regulación o protocolos.	☐	☐	☐	☐
08	Incidentes, casi incidentes y consultas alimentan la revisión de contenidos y controles.	☐	☐	☐	☐
09	Se mide eficacia con señales útiles: errores evitados, dudas recurrentes, uso no autorizado o calidad de revisión.	☐	☐	☐	☐
10	Dirección o el órgano responsable revisa periódicamente el programa y cierra acciones pendientes.	☐	☐	☐	☐

● La Comisión Europea indica que no se exige un certificado específico: un registro interno de formación y otras iniciativas puede servir de evidencia.

05 · ACTIVACIÓN

Plan de 30 días

Convierte el diagnóstico en cuatro entregables pequeños, asignados y verificables.

SEMANA	RESULTADO ESPERADO	RESPONSABLE	EVIDENCIA / FECHA
01	Inventario inicial, roles y colectivos alcanzados		
02	Política, herramientas permitidas y canal de consulta		
03	Formación común y módulos de mayor exposición		
04	Evaluación, refuerzos y revisión de dirección		

Matriz mínima de responsabilidades

ROL	DEBE PODER DEMOSTRAR
Dirección	Prioridad, recursos y revisión del riesgo aceptado.
Responsable de IA / cumplimiento	Inventario, criterios, evidencias, consultas y escalado.
IT y seguridad	Validación técnica, accesos, integración, registros e incidentes.
RR. HH. / formación	Colectivos, convocatorias, finalización, evaluación y refuerzos.
Responsables y personas usuarias	Aplicar el protocolo, revisar salidas y comunicar dudas o incidentes.

Evidencias y fuentes

Registra la evidencia sin convertir el proceso en burocracia. Una referencia clara debe permitir encontrar el documento y saber quién lo mantiene.

ID	EVIDENCIA	VERSIÓN / FECHA	RESPONSABLE	UBICACIÓN

Fuentes oficiales consultadas

Reglamento (UE) 2024/1689 · AI Act

eur-lex.europa.eu

Comisión Europea · Preguntas y respuestas sobre alfabetización en IA

digital-strategy.ec.europa.eu

Reglamento (UE) 2026/1744 · actualización del AI Act

eur-lex.europa.eu · DOUE-L-2026-81147

Aviso: recurso orientativo, no asesoramiento jurídico. Verifica la versión vigente del AI Act, sus actos de aplicación y la normativa sectorial antes de adoptar decisiones.