Guía de cumplimiento de IA 2026

Guía de cumplimiento de IA para empresas y particulares (2026): AI Act, DSA y RGPD

> **Qué es esto.** Un dossier práctico y verificado sobre lo que las autoridades europeas y españolas van a exigir a cualquiera que use inteligencia artificial, tenga una web o trate datos. Está pensado para que un empresario, un autónomo o un particular sepa qué le aplica, qué van a mirar con lupa los reguladores, dónde están las trampas y cómo prepararse sin gastar de más ni asustarse de menos.
>
> **Aviso.** Esto es información rigurosa, no asesoramiento jurídico individual. El marco legal de 2026 está en movimiento (lo señalamos donde toca). Cierre de esta edición: junio de 2026.

---

1. TL;DR: ¿esto me afecta?

Respuesta corta: **casi seguro que sí, pero probablemente menos de lo que temes y de otra forma de la que crees.**

- **¿Usas IA en tu empresa** (un chatbot, una herramienta que redacta, que puntúa currículums, que genera imágenes)? Te aplica el **Reglamento Europeo de IA (AI Act)**, casi siempre en su versión más ligera, y el **RGPD** si esa IA toca datos personales.
- **¿Tienes una web o app donde otros publican** (comentarios, reseñas, un marketplace, un foro)? Te aplica el **Reglamento de Servicios Digitales (DSA)**, normalmente solo en sus obligaciones básicas.
- **¿Eres autónomo o profesional y creas contenido con IA** (vídeos, voces, imágenes)? Te aplican las **obligaciones de transparencia** (revelar que es contenido sintético). En **uso puramente personal y no profesional**, el AI Act no te impone esas obligaciones de “responsable del despliegue”, pero siguen vigentes las prohibiciones y otras normas (derechos de autor, honor, protección de datos).

Las tres normas conviven y se complementan. No eliges una: te aplican las que correspondan a la vez. El resto del dossier es el mapa para saber cuáles y qué hacer.

---

2. El marco en una página

Norma	Qué regula	A quién apunta sobre todo
AI Act (Reglamento UE 2024/1689)	El **uso y la comercialización de sistemas de IA**, por niveles de riesgo	Quien fabrica IA (proveedor) y quien la usa profesionalmente (responsable del despliegue)
DSA (Reglamento UE 2022/2065)	Los **servicios digitales intermediarios** y la moderación de contenidos de terceros	Hostings, marketplaces, plataformas, buscadores
RGPD (Reglamento UE 2016/679)	El **tratamiento de datos personales** (también cuando lo hace una IA)	Cualquiera que trate datos de personas

Idea clave: el **AI Act** mira *qué hace el sistema de IA*; el **RGPD** mira *qué datos personales toca*; el **DSA** mira *qué pasa con el contenido que suben terceros a tu servicio*. Un mismo proyecto puede activar las tres.

---

3. La línea de tiempo (y el plazo que se movió)

El AI Act se aplica de forma **escalonada** (artículo 113). Lo que ya es obligatorio y exigible:

Fecha	Qué entra en juego	Estado
1 ago 2024	Entrada en vigor	Sin obligaciones aún
2 feb 2025	**Prácticas prohibidas (art. 5)** + **alfabetización en IA (art. 4)**	✅ En vigor y exigible
2 ago 2025	Obligaciones de **modelos de propósito general (GPAI)**, gobernanza y **régimen sancionador (arts. 99-100)**	✅ En vigor
2 ago 2026	**Alto riesgo del Anexo III** + **transparencia (art. 50)** + evaluaciones de impacto + sandboxes	Fecha por defecto
2 ago 2027	Alto riesgo integrado en **productos regulados (Anexo I)**	Fecha por defecto

> 🔴 **Caja: el plazo que se movió**
>
> Aquí está el matiz que casi nadie cuenta bien. La Comisión Europea propuso en noviembre de 2025 el **"Digital Omnibus"** (COM(2025)836), un paquete que **propone retrasar la entrada en vigor del régimen de alto riesgo**:
>
> - **Anexo III** (biometría, empleo, educación, servicios esenciales, etc.): del 2 ago 2026 a **finales de 2027** (las fuentes apuntan al 2 dic 2027).
> - **Anexo I** (IA dentro de productos regulados): del 2 ago 2027 a **2028** (en torno al 2 ago 2028).
>
> Pero ojo: a junio de 2026 esto es una **propuesta en tramitación legislativa** (procedimiento 2025/0359(COD)), **no derecho vigente**: el texto aún no se ha adoptado de forma definitiva ni publicado en el Diario Oficial de la UE, y las fechas exactas pueden cambiar durante la negociación. El Omnibus "mueve el reloj, no la arquitectura": no cambia las obligaciones de fondo, solo cuándo empiezan.
>
> **Qué hacer con esto:** planifica de forma conservadora hacia agosto de 2026, porque el retraso aún no es seguro, pero gana margen sabiendo que probablemente tendrás más tiempo del que dice el calendario por defecto. Verifica la fecha definitiva antes de tomar decisiones grandes. Fuente: Digital Omnibus, Comisión Europea.

Lo realmente importante para hoy: **las prohibiciones y la obligación de formación ya están en vigor desde febrero de 2025.** No son futuro.

---

4. AI Act por niveles de riesgo

El AI Act clasifica los sistemas de IA en cuatro niveles. Tu primera tarea es saber en cuál cae cada herramienta que usas.

🚫 Riesgo inaceptable (prohibido), art. 5

Ocho prácticas prohibidas desde febrero de 2025, sin posible mitigación. Las que más afectan a empresas:

- Manipulación subliminal o aprovechamiento de vulnerabilidades para alterar el comportamiento de forma perjudicial.
- **Puntuación social** (social scoring) de personas.
- **Reconocimiento de emociones en el trabajo y en centros educativos** (salvo razones médicas o de seguridad).
- **Categorización biométrica** por características sensibles (raza, religión, orientación, etc.).
- Creación de bases de datos de reconocimiento facial por **scraping masivo** de internet o cámaras.

Si alguna herramienta de tu empresa hace algo de esto, no se “mitiga”: se retira.

⚠️ Alto riesgo (Anexo III + Anexo I)

Sistemas en ocho ámbitos sensibles: biometría, infraestructuras críticas, **educación**, **empleo y RRHH** (cribado de currículums, decisiones de promoción), servicios esenciales (incluido **scoring crediticio**), aplicación de la ley, migración y justicia. Si fabricas uno, las obligaciones son fuertes: gestión de riesgos, gobernanza de datos, documentación técnica, registro de logs, supervisión humana, robustez, evaluación de conformidad, **marcado CE** y registro en una base de datos de la UE.

Si solo lo usas (eres “responsable del despliegue”), tus obligaciones son más acotadas pero reales: usarlo según las instrucciones, **supervisión humana** designada, conservar **logs (mínimo 6 meses)**, **informar a los representantes de los trabajadores** y, en ciertos casos, hacer una **evaluación de impacto en los derechos fundamentales (FRIA, art. 27)**.

💬 Riesgo limitado (transparencia), art. 50

El nivel donde caerá la mayoría de las pymes. Obligación principal: **avisar**.

- Un **chatbot** debe identificarse como IA (“hablas con un asistente automático”).
- Quien **fabrica** un sistema que genera contenido sintético debe marcarlo en formato legible por máquina (art. 50.2). Quien **publica un deepfake** debe **revelar que ha sido generado o manipulado con IA** (art. 50.4), con matices para obras creativas, satíricas o artísticas.

Estas obligaciones de transparencia se aplican desde **agosto de 2026**. Ojo: el retraso del Digital Omnibus afecta al **régimen de alto riesgo** (capítulo III), no a estas obligaciones del art. 50 (salvo una transición concreta para sistemas generativos ya en el mercado). Adelantarlas es buena práctica y a menudo ya lo exige la normativa de consumidores.

✅ Riesgo mínimo

Filtros antispam, videojuegos, recomendadores triviales. Sin obligaciones específicas del AI Act.

> **Modelos de propósito general (GPAI):** si usas ChatGPT, Claude, Gemini o similares, *tú* no eres su proveedor, así que las obligaciones GPAI (documentación técnica, resumen de datos de entrenamiento, política de derechos de autor; y para los más potentes, red-teaming y reporte de incidentes) recaen en la empresa que los fabrica, no en ti. A ti te afecta como *deployer* del nivel que corresponda al uso.

---

5. DSA: ¿tengo una “plataforma”? (y por qué probablemente no)

El DSA asusta más de lo que debe a las pymes. Lo que de verdad importa:

- **Web corporativa sin contenido de terceros:** el DSA **no te aplica**, porque no eres un “servicio intermediario” (el DSA solo regula a quien aloja o transmite contenido de terceros). Tus obligaciones vienen del RGPD y de la normativa de consumidores, no del DSA.
- **Web con comentarios o reseñas:** te conviertes en “hosting”. Obligaciones básicas: **mecanismo de notificación y retirada de contenido ilícito** (notice & action, art. 16) y **motivar** cuando eliminas algo (art. 17).
- **Marketplace o foro:** eres “plataforma en línea”, pero aquí está el alivio: el **artículo 19 exime a microempresas y pequeñas empresas** (menos de 50 empleados y menos de 10 M€) de las obligaciones más pesadas (sistema formal de reclamaciones, resolución extrajudicial, informes de transparencia). **No te exime** del notice & action ni de motivar las retiradas.
- **Plataforma muy grande (VLOP):** desde 45 millones de usuarios en la UE. Auditorías, evaluación de riesgos, supervisión directa de la Comisión. No es tu caso si lees esto.

Sanciones: hasta el **6% de la facturación mundial anual** (art. 74). Para las grandes plataformas (VLOP) las impone la Comisión Europea; para el resto de servicios intermediarios, las fijan las autoridades nacionales (art. 52), también hasta ese 6%. El DSA se aplica **plenamente desde el 17 de febrero de 2024**.

> **Dato que casi nadie cuenta:** en España, la autoridad del DSA es la **CNMC** (Coordinador de Servicios Digitales), pero la Comisión Europea **demandó a España ante el Tribunal de Justicia de la UE en mayo de 2025** (IP/25/1081) porque la CNMC todavía **no tiene plenas potestades sancionadoras**. El DSA es directamente aplicable igualmente, pero el régimen administrativo de multas en España está pendiente. Traducción: la obligación existe, el palo nacional todavía se está montando.

No confundas el DSA con el RGPD (datos) ni con el DMA (grandes plataformas y competencia): son normas distintas.

---

6. Quién vigila y qué van a mirar con lupa

Autoridades:

Autoridad	Ámbito
AI Office (Comisión Europea)	Modelos de propósito general (GPAI); coordinación UE
AESIA (Agencia Española de Supervisión de la IA, A Coruña)	Prácticas prohibidas, alto riesgo general, transparencia
AEPD	Datos personales, **biometría**, decisiones automatizadas (art. 22 RGPD)
CNMC	DSA y dimensión competitiva de los algoritmos

La AESIA existe y está operativa (creada por el RD 729/2023), y ya cerró el **primer sandbox regulatorio de IA de la UE**. Su potestad sancionadora plena depende de la futura **Ley Orgánica española de buen uso y gobernanza de la IA**, que a junio de 2026 sigue **en tramitación, no en vigor**.

Focos de fiscalización (lo que primero van a mirar):

1. Prácticas **prohibidas** (scoring social, biometría, manipulación). Ya sancionable.
2. **Transparencia**: chatbots y deepfakes sin avisar.
3. Sistemas de **alto riesgo sin conformidad** (RRHH, scoring) sin documentación ni supervisión humana.
4. **Intersección con el RGPD**: base legal, decisiones automatizadas, evaluaciones de impacto.
5. **Reclamaciones de afectados**: a menudo, la inspección empieza por una queja.

---

7. Sanciones: cuánto duele

AI Act (art. 99), cifras verificadas:

Conducta	Régimen general (el importe mayor)	Pymes (el importe menor)
Prácticas prohibidas (art. 5)	**35 M€ o 7%** de la facturación mundial	el menor de los dos
Incumplir otras obligaciones	**15 M€ o 3%**	el menor de los dos
Dar información incorrecta a las autoridades	**7,5 M€ o 1%**	el menor de los dos

Dos matices importantes y poco conocidos: el tramo de información incorrecta es del **1%** (no 1,5%, como repiten algunas fuentes), y para **pymes y startups se aplica el importe más bajo** de los dos (al revés que para las grandes). Detalle en el artículo 99.

DSA: hasta el **6%** de la facturación mundial anual (la Comisión Europea para las grandes plataformas; las autoridades nacionales para el resto de servicios intermediarios).

RGPD: hasta **20 M€ o el 4%**. En España, la AEPD resolvió en 2024 cientos de procedimientos sancionadores; la IA figura entre sus retos declarados.

---

8. Las trampas (errores típicos que se sancionan)

Ordenadas por gravedad regulatoria:

1. **IA en RRHH sin evaluación.** Cribar currículums o decidir promociones con IA es alto riesgo: exige base legal, evaluación de impacto y supervisión. Hacerlo a ciegas es triple infracción.
2. **Decisiones automatizadas sin intervención humana real** (art. 22 RGPD). El humano debe poder entender y anular el sistema, no firmar lo que diga la máquina.
3. **Biometría sin base legal reforzada** (art. 9 RGPD). En el ámbito laboral, en España el consentimiento del empleado no se considera válido por la relación de poder.
4. **Chatbot que no avisa de que es IA** (art. 50).
5. **Usar una IA de terceros sin contrato de encargado de tratamiento (DPA) firmado** antes de meterle datos personales. La responsabilidad recae en ti, no en el proveedor.
6. **Scraping masivo de datos personales para IA** sin test de ponderación. La Opinión 28/2024 del Comité Europeo de Protección de Datos es clara: el interés legítimo no gana automáticamente.
7. **Deepfakes y contenido sintético sin etiquetar.**
8. **No informar a la plantilla** de un uso de IA que les afecta (art. 64 del Estatuto de los Trabajadores + arts. 13-14 RGPD).
9. **"IA-washing"**: vender capacidades que el sistema no tiene (publicidad desleal).
10. **Copiar la política de IA de otra empresa.** Incumple el principio de responsabilidad proactiva y agrava la sanción si hay inspección.

---

9. Buenas vs malas prácticas

Aspecto	Mal	Bien
Inventario de IA	Informal, “ya sé lo que uso”	Registro con proveedor, finalidad, datos y base legal por herramienta
Decisiones automáticas	Sin revisión humana posible	Persona designada que puede anular + canal de impugnación visible
Chatbot	Se presenta como persona	“Soy un asistente de IA” desde el primer mensaje
Contenido con IA	Sin etiqueta	Etiqueta visible + marcado técnico en metadatos
Proveedor IA	API sin DPA firmado	DPA firmado antes de la primera llamada con datos personales
Formación	“Ya saben usar IA”	Registro firmado, proporcional al riesgo, actualizado
Supervisión	“El sistema es muy bueno”	Persona que entiende y puede anular; documentado
Incidentes	Esperar la queja del cliente	Protocolo: detectar, evaluar, notificar a la AEPD en 72 h

El hilo conductor es el **principio de responsabilidad proactiva (accountability)**: no basta con cumplir, hay que **poder demostrarlo y justificarlo** ante la autoridad con documentación viva.

---

10. Cómo preparar tu empresa: checklist por fases

Bloque A. Inventario (hazlo ya). Lista de toda herramienta de IA que usas: proveedor, para qué, qué datos toca, base legal y si tiene DPA firmado.

Bloque B. Base legal y contratos (antes de tratar datos). Una base legal del RGPD (art. 6) por cada tratamiento; **DPA firmado** con cada proveedor de IA (OpenAI, Anthropic y Google lo ofrecen); comprueba el mecanismo de transferencia internacional (marco UE-EE.UU. o cláusulas contractuales tipo).

Bloque C. Evaluaciones de impacto (antes de desplegar). Haz una **DPIA** si hay perfilado, categorías especiales o decisiones automatizadas significativas. Añade una **FRIA** (art. 27) si eres **organismo público**, una **entidad privada que presta servicios públicos**, o usas IA de alto riesgo para **evaluar la solvencia o el scoring crediticio** de personas o para **seguros de vida y salud** (Anexo III.5).

Bloque D. Transparencia (antes de agosto de 2026). Aviso de “hablas con IA” en chatbots; etiqueta del contenido generado con IA; mecanismo para impugnar decisiones automatizadas.

Bloque E. Formación (art. 4, ya en vigor). Formación documentada y firmada por empleado, proporcional al riesgo de su puesto. No exige certificación oficial, pero sí dejar constancia.

Bloque F. Supervisión y registros (continuo). Logs de decisiones, supervisión humana real documentada, revisión anual del inventario y protocolo de incidentes (notificación a la AEPD en 72 h si hay brecha).

---

11. Para particulares y autónomos

No solo las empresas están en el radar:

- **Creadores de contenido con IA (a título profesional):** la obligación de **revelar el contenido sintético** (art. 50) te alcanza cuando publicas deepfakes, voces o imágenes generadas en el marco de una actividad profesional. El uso puramente personal y doméstico queda en gran medida fuera del AI Act, aunque no de otras normas.
- **Deepfakes sin consentimiento:** además de la transparencia, ciertos usos (sexuales, suplantación) están prohibidos o tipificados. La futura ley española refuerza esto.
- **Derechos de autor:** generar con IA no te da automáticamente la titularidad, y usar obras ajenas para crear puede tener consecuencias.
- **Autónomos que usan IA con datos de clientes:** te aplican las mismas reglas de RGPD y de DPA con el proveedor que a una empresa.

---

12. Glosario rápido

- **Proveedor:** quien fabrica o comercializa el sistema de IA.
- **Responsable del despliegue (deployer):** quien usa el sistema de IA en su actividad. La mayoría de las empresas.
- **GPAI:** modelo de IA de propósito general (los grandes modelos generativos).
- **DPIA:** evaluación de impacto en protección de datos (RGPD, art. 35).
- **FRIA:** evaluación de impacto en los derechos fundamentales (AI Act, art. 27).
- **DPA:** contrato de encargado de tratamiento (RGPD, art. 28).
- **VLOP:** plataforma en línea muy grande (DSA).
- **Accountability:** responsabilidad proactiva, poder demostrar el cumplimiento.

Fuentes

> Para los números de artículo y las sanciones, la fuente que manda es siempre el **texto oficial en EUR-Lex / DOUE**. Las páginas de análisis (como artificialintelligenceact.eu) se incluyen solo como apoyo divulgativo, no como fuente normativa.

Primarias (AI Act) - Reglamento (UE) 2024/1689, texto consolidado (incluye arts. 5, 27, 50, 99 y 113): https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es - Calendario de aplicación (AI Act Service Desk, Comisión Europea): https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act - Digital Omnibus, propuesta COM(2025)836 (Comisión Europea): https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

Apoyo divulgativo (no oficial) - AI Act Explorer (análisis por artículos, arts. 27/50/99): https://artificialintelligenceact.eu/es/

DSA - Reglamento (UE) 2022/2065, texto en español: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32022R2065 - Política DSA (Comisión Europea): https://digital-strategy.ec.europa.eu/en/policies/digital-services-act - Lista de VLOP/VLOSE: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops - CNMC, Coordinador de Servicios Digitales: https://www.cnmc.es/en/sectores-que-regulamos/servicios-digitales-dsa - Demanda de la Comisión a España (IP/25/1081): https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

España / RGPD - AESIA (web oficial): https://aesia.digital.gob.es/es - RD 729/2023 (estatuto AESIA): https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911 - AEPD, guía de adecuación al RGPD de tratamientos con IA: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf - AEPD, orientaciones sobre IA agéntica: https://www.aepd.es/guias/orientaciones-ia-agentica.pdf - EDPB, Opinión 28/2024 (modelos de IA y protección de datos): https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

Casos - Multa del Garante italiano a OpenAI (15 M€, diciembre 2024). Fuente primaria: comunicado del *Garante per la protezione dei dati personali* (https://www.garanteprivacy.it). Cobertura de prensa (secundaria): https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection

Edición cerrada en junio de 2026. El marco normativo está en evolución (en particular, el Digital Omnibus y la ley orgánica española de IA). Verifica las fechas y el estado de tramitación antes de tomar decisiones con impacto legal. Información general, no asesoramiento jurídico individual.