Europa modifica el AI Act y aplaza parte de las obligaciones para los sistemas de inteligencia artificial de alto riesgo

El nuevo Reglamento Ómnibus Digital sobre Inteligencia Artificial amplía determinados plazos, simplifica algunas obligaciones y refuerza la supervisión, pero no establece una moratoria general del AI Act

Por Iván Martínez, CEO de Intedya

La Unión Europea acaba de introducir la primera gran reforma del Reglamento de Inteligencia Artificial desde su aprobación. El Diario Oficial de la Unión Europea ha publicado el Reglamento (UE) 2026/1744, de 8 de julio de 2026, conocido como Ómnibus digital sobre inteligencia artificial, mediante el que se modifican el AI Act, el Reglamento europeo de aviación civil y el Reglamento de Máquinas. La nueva norma tiene como objetivo simplificar la aplicación del marco europeo de inteligencia artificial, reducir duplicidades y facilitar el cumplimiento sin rebajar la protección de la salud, la seguridad y los derechos fundamentales. La reforma llega después de meses de debate sobre la falta de normas armonizadas, especificaciones técnicas, orientaciones y organismos preparados para aplicar determinadas obligaciones del Reglamento de Inteligencia Artificial. La noticia más visible es el aplazamiento de los requisitos aplicables a determinados sistemas de IA de alto riesgo. Sin embargo, interpretar esta modificación como una suspensión general del AI Act sería un error.

Europa ha concedido más tiempo para cumplir algunas obligaciones de alto riesgo, pero el Reglamento de Inteligencia Artificial continúa plenamente vigente y muchas de sus disposiciones ya son exigibles.

El Reglamento de Inteligencia Artificial entró en vigor el 1 de agosto de 2024 y estableció un calendario de aplicación progresiva. Durante los primeros meses de implantación, las instituciones europeas y los operadores económicos han identificado dificultades relevantes: retrasos en el desarrollo de normas armonizadas, falta de criterios técnicos suficientemente detallados, estructuras nacionales de supervisión todavía incompletas y riesgo de duplicación con otras legislaciones sectoriales. El propio Reglamento reconoce que estos retrasos podían generar una carga regulatoria superior a la inicialmente prevista y dificultar una aplicación sencilla, uniforme y efectiva del AI Act. No obstante, la reforma insiste en que las medidas de simplificación no deben reducir el nivel de protección de la salud, la seguridad ni los derechos fundamentales. El Ómnibus Digital pretende, por tanto, corregir problemas de ejecución sin alterar la filosofía esencial de la regulación europea: una inteligencia artificial centrada en las personas, fiable y gestionada conforme a un enfoque basado en riesgos.

El nuevo calendario para los sistemas de IA de alto riesgo

La modificación más relevante afecta a las fechas de aplicación de las obligaciones previstas para los sistemas de inteligencia artificial clasificados como de alto riesgo.

El nuevo calendario distingue dos grandes categorías.

2 de diciembre de 2027: sistemas de alto riesgo del Anexo III

Las obligaciones del capítulo III, secciones 1, 2 y 3, serán aplicables desde el 2 de diciembre de 2027 para los sistemas clasificados como de alto riesgo conforme al artículo 6.2 y el Anexo III del AI Act.

En este grupo se encuentran determinados sistemas utilizados en ámbitos especialmente sensibles, entre ellos:

- Biometría.
- Educación y formación profesional.
- Selección, contratación y gestión de trabajadores.
- Acceso a servicios privados y públicos esenciales.
- Evaluación crediticia y determinados servicios financieros.
- Migración, asilo y control de fronteras.
- Administración de justicia.
- Procesos democráticos y determinados usos en el sector público.

No todos los sistemas utilizados en estos ámbitos son automáticamente de alto riesgo. La clasificación dependerá de su finalidad, contexto, funcionamiento y de las excepciones establecidas en el propio Reglamento.

2 de agosto de 2028: sistemas de alto riesgo vinculados a productos regulados

Las obligaciones serán aplicables desde el 2 de agosto de 2028 para los sistemas clasificados como de alto riesgo conforme al artículo 6.1 y el Anexo I.

Se trata, fundamentalmente, de sistemas de IA que constituyen un producto regulado por determinada legislación europea o que funcionan como componente de seguridad de dicho producto.

Esta categoría puede afectar, entre otros, a productos sanitarios, vehículos, ascensores, equipos de protección, juguetes, equipos radioeléctricos y otros productos sometidos a legislación europea de armonización y, en ciertos casos, a evaluación de conformidad.

El nuevo Reglamento establece expresamente estas dos fechas: 2 de diciembre de 2027 para los sistemas de alto riesgo del Anexo III y 2 de agosto de 2028 para los sistemas vinculados a productos del Anexo I.

No existe una moratoria general del AI Act

El aplazamiento afecta a determinados requisitos de los sistemas de alto riesgo, pero no paraliza el Reglamento de Inteligencia Artificial.

Esta es, probablemente, la principal confusión que deben evitar las organizaciones.

El AI Act continúa aplicándose conforme a su calendario y siguen siendo relevantes, entre otras, las disposiciones relativas a:

- Prácticas de inteligencia artificial prohibidas.
- Obligaciones de los proveedores de modelos de IA de propósito general.
- Gobernanza y autoridades de supervisión.
- Alfabetización en materia de inteligencia artificial.
- Transparencia de determinados sistemas.
- Identificación y marcado de contenidos sintéticos.
- Responsabilidades contractuales entre proveedores tecnológicos.
- Obligaciones que no hayan sido expresamente aplazadas.
- Régimen sancionador y medidas de vigilancia del mercado.

Las empresas no pueden interpretar el nuevo calendario como una autorización para detener sus proyectos de cumplimiento.

Por el contrario, el tiempo adicional debería emplearse para completar inventarios, clasificar sistemas, asignar responsabilidades, revisar contratos, establecer controles y desarrollar una estructura real de gobernanza.

La alfabetización en IA no desaparece, pero cambia su formulación

Uno de los cambios más significativos afecta al artículo 4 del AI Act, relativo a la alfabetización en inteligencia artificial. La redacción anterior obligaba a proveedores y responsables del despliegue a garantizar un nivel suficiente de alfabetización de su personal. La nueva formulación exige que proveedores y responsables del despliegue adopten medidas para apoyar la promoción de la alfabetización en IA de las personas encargadas del funcionamiento y utilización de los sistemas. Estas medidas deberán adaptarse a:

- Los conocimientos técnicos de las personas.
- Su experiencia, educación y formación.
- El contexto previsto de utilización.
- Los sistemas de IA utilizados.
- Las personas o colectivos sobre los que puedan emplearse.

La norma aclara que la obligación no exige garantizar que cada persona alcance un nivel específico de conocimiento. Sin embargo, esto no elimina la necesidad de formar, sensibilizar y capacitar al personal. El nuevo artículo 4 mantiene una obligación organizativa concreta: adoptar y poder demostrar medidas razonables y proporcionadas de alfabetización en IA. Por tanto, cancelar los programas de formación sería una decisión difícilmente justificable. Lo razonable será revisar su alcance y vincularlos al riesgo, a las funciones de cada persona y al uso efectivo de los sistemas.

Nuevas prácticas prohibidas: imágenes íntimas y material de abuso sexual de menores

La reforma no se limita a simplificar obligaciones. También amplía expresamente el catálogo de prácticas prohibidas. El nuevo Reglamento incorpora la prohibición de introducir en el mercado, poner en servicio o utilizar determinados sistemas de IA que generen o manipulen imágenes, vídeos, audios u otros contenidos realistas de carácter íntimo de una persona identificable sin su consentimiento. También se prohíben determinados sistemas destinados a generar o manipular material relacionado con abusos sexuales de menores. La prohibición afecta tanto a los sistemas específicamente diseñados para producir este contenido como a aquellos en los que dicho resultado sea razonablemente previsible y reproducible y no existan medidas de seguridad adecuadas. Para los responsables del despliegue, la prohibición opera cuando el sistema se utiliza con la finalidad de generar o manipular ese material. Estas nuevas prohibiciones serán aplicables desde el 2 de diciembre de 2026. La modificación supone una respuesta directa al crecimiento de las herramientas de “nudificación”, los contenidos íntimos sintéticos no consentidos y otras formas de abuso facilitadas mediante IA generativa.

Cambios en las obligaciones de transparencia sobre contenidos sintéticos

La reforma también introduce un periodo transitorio para determinados proveedores de sistemas de IA generativa. Los proveedores de sistemas, incluidos los sistemas basados en modelos de propósito general, que generen audio, imagen, vídeo o texto sintético y que ya estuvieran en el mercado antes del 2 de agosto de 2026 deberán adoptar las medidas necesarias para cumplir las obligaciones de marcado del artículo 50.2 a más tardar el 2 de diciembre de 2026. Esta obligación resulta especialmente relevante para plataformas, desarrolladores de herramientas generativas y empresas que comercializan o integran sistemas capaces de producir contenidos artificiales. Las organizaciones deberán revisar no solo el contenido visible para el usuario, sino también los mecanismos técnicos de marcado, trazabilidad, etiquetado y detección.

Mayor proporcionalidad para pymes y empresas de mediana capitalización

El Reglamento amplía varias medidas de simplificación destinadas inicialmente a microempresas. Las pymes, incluidas las empresas emergentes, podrán cumplir de manera simplificada determinados elementos del sistema de gestión de la calidad exigido a los proveedores de sistemas de alto riesgo. También se prevén formularios simplificados de documentación técnica y una aplicación proporcional de determinados requisitos atendiendo al tamaño y recursos de la organización.

La reforma extiende además determinados beneficios a las denominadas pequeñas empresas de mediana capitalización o small mid-caps, empresas que superan los umbrales de pyme, pero que siguen enfrentándose a dificultades similares en materia de costes y carga administrativa. Estas medidas no implican una exención de cumplimiento. La simplificación debe conservar el nivel de protección exigido y el grado de rigor necesario para demostrar la conformidad de los sistemas de alto riesgo.

Una definición más precisa de “componente de seguridad”

El Ómnibus Digital modifica la definición de componente de seguridad, un concepto esencial para determinar cuándo un sistema integrado en un producto debe clasificarse como de alto riesgo. La nueva regulación aclara que un sistema cumple una función de seguridad cuando su finalidad prevista consiste en prevenir o mitigar riesgos para la salud y la seguridad de las personas o de los bienes. No se considerarán componentes de seguridad los sistemas utilizados únicamente para:

- Asistencia al usuario.
- Optimización del rendimiento.
- Eficiencia del servicio.
- Automatización.
- Comodidad.
- Control de calidad no relacionado con la seguridad.

Sin embargo, cuando el fallo o funcionamiento defectuoso del sistema pueda poner en peligro la salud o la seguridad, sí podrá ser considerado componente de seguridad. Esta precisión reducirá clasificaciones excesivamente amplias, pero obligará a documentar cuidadosamente la finalidad prevista, los modos de fallo y las consecuencias razonablemente previsibles.

Sistemas de IA ya existentes: importancia de las modificaciones significativas

El nuevo Reglamento aclara el tratamiento de los sistemas de alto riesgo introducidos en el mercado o puestos en servicio antes de las nuevas fechas de aplicación. Como regla general, el AI Act se aplicará a estos sistemas cuando, después de la fecha correspondiente, sean objeto de cambios significativos en su diseño. La norma aclara además que, cuando una unidad de un determinado tipo y modelo se haya introducido legalmente en el mercado, otras unidades del mismo tipo podrán beneficiarse del régimen transitorio siempre que su diseño permanezca inalterado. Esto hace especialmente importante controlar y documentar:

- La fecha de primera introducción en el mercado.
- Las versiones del sistema.
- Los cambios en algoritmos y modelos.
- Las modificaciones de datos o funcionalidades.
- Las ampliaciones de finalidad.
- Las actualizaciones que puedan considerarse sustanciales.

Una actualización aparentemente ordinaria podría desencadenar la aplicación plena de las obligaciones si altera de forma significativa el diseño, la finalidad o el comportamiento del sistema.

Más obligaciones contractuales en la cadena tecnológica

La reforma refuerza también la cooperación entre los distintos operadores de la cadena de suministro. Cuando un tercero suministre modelos, herramientas, servicios, componentes o procesos utilizados en un sistema de alto riesgo, deberá existir un acuerdo escrito que determine la información, las capacidades, el acceso técnico y la asistencia necesarios para permitir que el proveedor final cumpla sus obligaciones.

Estos acuerdos deberán contemplar aspectos como:

- Acceso a documentación técnica.
- Información sobre limitaciones y modos de fallo.
- Capacidades de prueba y validación.
- Asistencia para la evaluación de conformidad.
- Gestión de incidentes.
- Cooperación ante autoridades.
- Distribución de responsabilidades.
- Comunicación de cambios relevantes.

Los contratos tecnológicos genéricos serán insuficientes en muchos casos. Las organizaciones tendrán que incorporar cláusulas específicas de cumplimiento del AI Act.

Tratamiento de datos sensibles para detectar y corregir sesgos

La reforma incorpora una nueva base jurídica para el tratamiento excepcional de categorías especiales de datos personales cuando sea estrictamente necesario para detectar y corregir sesgos. Esta posibilidad está sometida a condiciones rigurosas, entre ellas:

- Que no sea posible alcanzar el objetivo con datos sintéticos o anonimizados.
- Aplicación de medidas avanzadas de seguridad y privacidad.
- Pseudonimización.
- Controles estrictos de acceso.
- Prohibición de transmisión a terceros.
- Eliminación de los datos una vez corregido el sesgo.
- Documentación de la necesidad del tratamiento.

La medida no crea una obligación general de utilizar datos sensibles para evaluar sesgos, pero proporciona una base jurídica excepcional cuando ese tratamiento sea imprescindible. Las empresas deberán coordinar estas actividades con sus sistemas de protección de datos, evaluaciones de impacto, controles de seguridad y procedimientos de gobernanza.

Más poder para la Oficina Europea de Inteligencia Artificial

Otro de los grandes cambios es el refuerzo de la Oficina de IA. La Oficina tendrá competencia exclusiva sobre determinados sistemas basados en modelos de IA de propósito general, especialmente cuando el modelo y el sistema hayan sido desarrollados por el mismo proveedor o por empresas pertenecientes al mismo grupo. También asumirá competencias sobre sistemas integrados en plataformas en línea o motores de búsqueda considerados de muy gran tamaño.

Entre sus facultades se incluyen:

- Solicitar información.
- Acceder a sistemas y documentación.
- Realizar inspecciones a distancia o presenciales.
- Examinar datos, libros y registros.
- Exigir explicaciones.
- Ordenar medidas correctoras.
- Convertir compromisos empresariales en jurídicamente vinculantes.
- Imponer multas y multas coercitivas.
- Retirar o restringir sistemas del mercado.

La Oficina podrá imponer multas coercitivas diarias que, en determinados supuestos, podrán alcanzar el 5 % de los ingresos diarios medios o del volumen de negocios anual mundial del ejercicio anterior. La reforma confirma así que la simplificación regulatoria no equivale a una reducción de la capacidad de supervisión.

Espacios controlados de pruebas y experimentación en condiciones reales

El Reglamento amplía las posibilidades de probar sistemas de IA en espacios controlados y en condiciones reales. Los Estados miembros deberán garantizar que exista al menos un espacio controlado de pruebas operativo a más tardar el 2 de agosto de 2027. La Oficina de IA podrá crear además un espacio controlado de pruebas a escala europea, con acceso prioritario para pymes, empresas emergentes y pequeñas empresas de mediana capitalización.

También se amplía la posibilidad de realizar pruebas en condiciones reales para determinados sistemas de alto riesgo, siempre que se establezcan planes, mecanismos de supervisión y garantías suficientes.

Estas medidas pretenden facilitar la innovación, pero no eliminan la necesidad de gestionar riesgos, proteger datos personales y garantizar los derechos de las personas participantes.

La oportunidad y el riesgo para las organizaciones

El nuevo calendario ofrece un margen adicional para implantar los requisitos más complejos de los sistemas de alto riesgo. Pero este margen puede interpretarse de dos maneras. Una organización puede utilizarlo para retrasar decisiones, mantener sistemas sin inventariar y confiar en que aparezcan nuevas prórrogas. O puede aprovecharlo para construir un sistema de gobernanza sólido antes de que las obligaciones sean plenamente exigibles. La segunda opción es la única razonable desde una perspectiva de cumplimiento, gestión de riesgos y responsabilidad corporativa. Clasificar un sistema, completar su documentación técnica, establecer un sistema de gestión de riesgos, garantizar la calidad de los datos, implantar supervisión humana, revisar contratos y crear mecanismos de vigilancia poscomercialización requiere meses de trabajo, En organizaciones complejas, puede requerir años.

Decálogo urgente para adaptarse al nuevo Ómnibus Digital

1. Actualizar el calendario interno del AI Act

Los planes de cumplimiento deben incorporar las nuevas fechas del 2 de diciembre de 2026, 2 de diciembre de 2027 y 2 de agosto de 2028, sin olvidar las obligaciones ya aplicables.

2. Inventariar todos los sistemas de inteligencia artificial

El inventario debe incluir herramientas corporativas, soluciones integradas en procesos, desarrollos internos, modelos generativos, sistemas contratados a terceros y aplicaciones utilizadas informalmente por el personal.

3. Determinar el rol de la organización

Es imprescindible establecer si la empresa actúa como proveedor, responsable del despliegue, importador, distribuidor, fabricante de producto o representante autorizado.

Una misma empresa puede desempeñar varios roles simultáneamente.

4. Identificar sistemas potencialmente de alto riesgo

La clasificación debe analizar la finalidad prevista, el sector, las personas afectadas, el grado de autonomía, las consecuencias de las decisiones y la relación con productos regulados.

5. Diferenciar los sistemas del Anexo III y los vinculados a productos

La distinción determina el calendario, las obligaciones y el procedimiento de evaluación de la conformidad.

6. Mantener los programas de gobernanza y alfabetización

La nueva redacción del artículo 4 no elimina la formación. Exige medidas adaptadas a los conocimientos, funciones y contexto de uso de las personas.

7. Revisar las obligaciones de transparencia

Deben analizarse los sistemas que interactúan con personas, reconocen emociones, generan contenidos sintéticos o producen imágenes, audio, vídeo o texto artificial.

8. Documentar los sistemas preexistentes y sus modificaciones

Es esencial conservar evidencias sobre fechas, versiones, cambios funcionales, actualizaciones y modificaciones del diseño.

9. Actualizar los contratos tecnológicos

Los acuerdos con proveedores deberán regular expresamente el acceso a documentación, datos, pruebas, limitaciones técnicas, incidentes, auditorías y responsabilidades.

10. Implantar un sistema de cumplimiento del AI Act

El cumplimiento no puede depender de acciones aisladas. Requiere una estructura permanente de políticas, funciones, controles, evidencias, evaluación de riesgos, formación, supervisión y mejora continua.

Conclusión: más tiempo, pero no menos responsabilidad

El Reglamento Ómnibus Digital supone una reforma de gran alcance. Europa reconoce que el calendario original de los sistemas de alto riesgo no era viable sin normas, orientaciones y estructuras de evaluación suficientemente desarrolladas. Por ese motivo, amplía determinados plazos, introduce simplificaciones y busca una mayor coordinación con la legislación sectorial. Pero la reforma no deroga ni suspende el AI Act. Las prácticas prohibidas siguen siendo exigibles. Las obligaciones de los modelos de propósito general continúan vigentes. La transparencia sobre contenidos sintéticos avanza. La alfabetización en IA sigue siendo necesaria. La supervisión se refuerza y la Oficina de IA recibe mayores competencias de investigación y sanción. La conclusión es clara, Europa concede más tiempo para determinadas obligaciones de los sistemas de alto riesgo, pero no concede una moratoria general para cumplir el Reglamento de Inteligencia Artificial. Las organizaciones que todavía no dispongan de un sistema de gobernanza y cumplimiento del AI Act deberían comenzar su implantación de inmediato.