



Inteligencia artificial: preguntas y respuestas*

Brussels, 1 de agosto de 2024

¿Por qué necesitamos regular el uso de la inteligencia artificial?

El Reglamento de Inteligencia Artificial de la UE es la primera ley integral en materia de inteligencia artificial del mundo. Su objetivo es tratar los riesgos para la salud, la seguridad y los derechos fundamentales. El Reglamento también protege la democracia, el Estado de Derecho y el medio ambiente.

La adopción de los sistemas de inteligencia artificial puede reportar importantes beneficios sociales, fomentar el crecimiento económico y mejorar la innovación en la UE y su competitividad a escala mundial. Sin embargo, hay casos en los que las características específicas de determinados sistemas de inteligencia artificial pueden dar lugar a nuevos riesgos relacionados con la seguridad, incluso física, y los derechos fundamentales. Algunos modelos potentes de inteligencia artificial ya ampliamente utilizados podrían incluso plantear riesgos sistémicos.

Esto da lugar a inseguridad jurídica y a una aceptación potencialmente más lenta de las tecnologías de inteligencia artificial por parte de las autoridades públicas, las empresas y los ciudadanos, debido a la falta de confianza. La disparidad de las respuestas normativas de las autoridades nacionales entrañaría el riesgo de fragmentar el mercado interior.

Para hacer frente a estos retos, es necesaria una acción legislativa que garantice el correcto funcionamiento del mercado interior de los sistemas de inteligencia artificial, con una ponderación adecuada de los beneficios y de los riesgos.

¿A quién se aplica el Reglamento de Inteligencia Artificial?

El marco normativo se aplicará a los agentes tanto públicos como privados, de dentro y fuera de la UE, en la medida en que el **sistema de inteligencia artificial** se introduzca en el mercado de la Unión o su uso afecte a personas establecidas en ella.

Las obligaciones pueden afectar tanto a los proveedores (por ejemplo, un programador de una herramienta de evaluación de resúmenes curriculares) como a los usuarios de sistemas de inteligencia artificial de alto riesgo (por ejemplo, un banco que compre esa herramienta). Existen algunas excepciones al Reglamento. Las actividades de investigación, desarrollo y creación de prototipos que tengan lugar antes de la comercialización de un sistema de inteligencia artificial no están sujetas a estas normas. Además, los sistemas de inteligencia artificial diseñados exclusivamente con fines militares, de defensa o de seguridad nacional también están exentos, independientemente del tipo de entidad que lleve a cabo esas actividades.

¿Cuáles son las categorías de riesgo?

El Reglamento de Inteligencia Artificial introduce un marco uniforme en todos los países de la UE, basado en una definición prospectiva de la inteligencia artificial y un enfoque basado en el riesgo:

- **Riesgo inadmisibles:** Se trata de un conjunto muy limitado de usos especialmente nocivos de la inteligencia artificial que se oponen a los valores de la UE porque vulneran los derechos fundamentales y, en consecuencia, quedarán prohibidos:
 - **aprovechamiento de los puntos vulnerables de las personas, manipulación y uso de técnicas subliminales;**
 - **puntuación social** con fines públicos y privados;
 - **actuación policial predictiva individual** basada únicamente en la elaboración de perfiles de personas;
 - **extracción no selectiva** de internet o circuito cerrado de televisión para imágenes faciales con el fin de crear o ampliar bases de datos;
 - **reconocimiento de emociones en el lugar de trabajo y en las instituciones**

educativas, a menos que sea por razones médicas o de seguridad (por ejemplo, control del grado de cansancio de un piloto);

- **categorización biométrica** de las personas físicas para deducir o inferir su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, u orientación sexual. El etiquetado o el filtrado de conjuntos de datos y la categorización de los datos en el ámbito policial seguirán siendo posibles;
- **identificación biométrica remota, en tiempo real, en lugares de acceso público por parte de la policía**, con excepciones limitadas (véase más adelante).
- La Comisión publicará directrices sobre las prohibiciones antes de su entrada en vigor el 2 de febrero de 2025.
- **Alto riesgo**: Se considera de alto riesgo un número limitado de sistemas de inteligencia artificial definidos en la propuesta y que tienen un impacto potencial negativo en la seguridad de las personas o en sus derechos fundamentales, tal y como están protegidos por la Carta de los Derechos Fundamentales de la UE. Se adjunta al Reglamento de Inteligencia Artificial la lista de sistemas de inteligencia artificial de alto riesgo, que puede revisarse para adaptarla a la evolución de la casuística práctica de la inteligencia artificial.
- Entre ellos figuran los componentes de seguridad de los productos contemplados en la legislación sectorial de la Unión. Siempre se considerarán de alto riesgo cuando estén sujetos a una evaluación de la conformidad por terceros con arreglo a esa legislación sectorial.
- Estos sistemas de inteligencia artificial de alto riesgo abarcan, por ejemplo, los sistemas de inteligencia artificial que evalúan si alguien puede recibir un determinado tratamiento médico u obtener un determinado empleo o préstamo para comprar un apartamento. Otros sistemas de inteligencia artificial de alto riesgo son los utilizados por la policía para elaborar perfiles de personas o evaluar su riesgo de cometer un delito (a menos que esté prohibido en virtud del artículo 5). También podrían ser de alto riesgo los sistemas de inteligencia artificial que hagan funcionar robots, drones o dispositivos médicos.
- **Riesgo específico de transparencia**: Para fomentar la confianza, es importante garantizar la transparencia en torno al uso de la inteligencia artificial. Por lo tanto, el Reglamento de Inteligencia Artificial establece obligaciones específicas de transparencia en el caso de determinadas aplicaciones de inteligencia artificial, por ejemplo, cuando exista un riesgo claro de manipulación (por ejemplo, mediante el uso de robots conversacionales) o ultrafalsificación. Los usuarios deben ser conscientes de que están interactuando con una máquina.
- **Riesgo mínimo**: La mayoría de los demás sistemas de inteligencia artificial puede programarse y utilizarse con arreglo a la legislación vigente, sin obligaciones jurídicas adicionales. De forma voluntaria, los proveedores de estos sistemas pueden optar por aplicar los requisitos de una inteligencia artificial digna de confianza y adherirse a códigos de conducta facultativos.

Además, el Reglamento de Inteligencia Artificial tiene en cuenta los **riesgos sistémicos** que podrían derivarse de los **modelos de inteligencia artificial de uso general**, incluidos los grandes **modelos generativos de inteligencia artificial**. Pueden utilizarse para diversas tareas y se están convirtiendo en la base de muchos sistemas de inteligencia artificial en la UE. Algunos de estos modelos podrían entrañar riesgos sistémicos si tienen gran capacidad o son objeto de un uso generalizado. Por ejemplo, los modelos potentes podrían causar accidentes graves o ser utilizados indebidamente para ciberataques de amplio alcance. Muchas personas podrían verse afectadas si un modelo propaga sesgos nocivos en múltiples aplicaciones.

¿Cómo se puede saber si un sistema de inteligencia artificial es de alto riesgo?

El Reglamento de Inteligencia Artificial establece una metodología sólida para clasificar como de alto riesgo sistemas de inteligencia artificial. El objetivo es aportar seguridad jurídica a las empresas y otros agentes económicos.

La clasificación del riesgo se basa en la finalidad prevista del sistema de inteligencia artificial, en consonancia con la legislación vigente de la UE en materia de seguridad de los productos. Esto significa que la clasificación del riesgo depende de la función desempeñada por el sistema de inteligencia artificial y de la finalidad y las modalidades concretas para las que se utilice dicho sistema.

Los sistemas de inteligencia artificial pueden clasificarse como de alto riesgo en dos casos:

- si el sistema de inteligencia artificial está integrado como componente de seguridad en productos contemplados en la legislación vigente sobre productos (anexo I) o constituye por sí

mismo uno de esos productos. Podría tratarse, por ejemplo, de programas informáticos de medicina basados en la inteligencia artificial.

- Si el sistema de inteligencia artificial está destinado a utilizarse en un caso de uso de alto riesgo que figure en el anexo III del Reglamento de Inteligencia Artificial. La lista abarca casos de uso en ámbitos como la educación, el empleo, la policía o la migración.

La Comisión está elaborando directrices para la clasificación de alto riesgo, que se publicarán antes de la fecha de aplicación de estas normas.

¿Cuáles son los ejemplos de casos de uso de alto riesgo definidos en el anexo III?

El anexo III comprende ocho ámbitos en los que el uso de la inteligencia artificial puede ser especialmente delicado y enumera casos de uso concretos para cada ámbito. Un sistema de inteligencia artificial se clasifica como de alto riesgo si está destinado a ser utilizado en uno de esos casos de uso.

Como ejemplos cabe mencionar:

- los sistemas de inteligencia artificial utilizados como elementos de seguridad en determinadas **infraestructuras críticas**, por ejemplo, en los ámbitos del tráfico por carretera y el suministro de agua, gas, calefacción y electricidad;
- **los sistemas de inteligencia artificial utilizados en la educación y la formación profesional**, por ejemplo, para evaluar los resultados de la enseñanza, dirigir el proceso de aprendizaje y controlar que no se hagan trampas;
- **los sistemas de inteligencia artificial utilizados en el empleo, la gestión del personal laboral** y el acceso al trabajo por cuenta propia, por ejemplo, para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos;
- **los sistemas de inteligencia artificial utilizados en el acceso a servicios y prestaciones públicos y privados esenciales** (por ejemplo, asistencia sanitaria), la **evaluación de la solvencia crediticia** y la evaluación de riesgos y la fijación de precios en relación con los **seguros de vida y de enfermedad**;
- los sistemas de inteligencia artificial utilizados en los ámbitos de la **policía**, la migración y el **control fronterizo**, en la medida en que no estén ya prohibidos, así como en la administración de **justicia** y los **procesos democráticos**;
- los sistemas de inteligencia artificial utilizados a efectos de **identificación biométrica, categorización biométrica y reconocimiento de emociones**, en la medida en que no estén prohibidos.

¿Cuáles son las obligaciones de los proveedores de sistemas de inteligencia artificial de alto riesgo?

Antes de **comercializar un sistema de inteligencia artificial de alto riesgo en el mercado de la Unión** o de ponerlo en servicio de otra forma, los proveedores deberán someterlo a una **evaluación de la conformidad**. Esto les permitirá demostrar que su sistema cumple los requisitos obligatorios de una inteligencia artificial digna de confianza (por ejemplo, calidad de los datos, documentación y trazabilidad, transparencia, supervisión humana, exactitud, ciberseguridad y solidez). Esta evaluación debe repetirse si el sistema o su finalidad se modifican sustancialmente.

Los sistemas de inteligencia artificial que sean elementos de seguridad de productos contemplados en la legislación sectorial de la Unión siempre se considerarán de alto riesgo cuando estén sujetos a una evaluación de la conformidad por terceros con arreglo a dicha legislación sectorial. Además, todos los sistemas biométricos, independientemente de su aplicación, requerirán una evaluación de la conformidad por terceros.

Los proveedores de sistemas de inteligencia artificial de alto riesgo también tendrán que **aplicar sistemas de gestión de la calidad y los riesgos** para garantizar su conformidad con los nuevos requisitos y reducir al mínimo los riesgos para los usuarios y las personas afectadas, incluso después de que los productos se hayan comercializado.

Los sistemas de inteligencia artificial de alto riesgo utilizados por las autoridades públicas o las entidades que actúen en su nombre deberán **registrarse en una base de datos pública de la UE**, a menos que tales sistemas se empleen con fines policiales y de migración. Estos últimos usos tendrán que registrarse en una parte no pública de la base de datos, a la que solo podrán acceder las autoridades de supervisión pertinentes.

Para garantizar el cumplimiento a lo largo de todo el ciclo de vida del sistema de inteligencia artificial, las autoridades de vigilancia del mercado efectuarán periódicamente auditorías y facilitarán el seguimiento posterior a la comercialización; también permitirán a los proveedores denunciar voluntariamente cualquier incidente grave o incumplimiento de las obligaciones en materia de derechos fundamentales que lleguen a su conocimiento. En casos excepcionales, las autoridades podrán conceder excepciones a la introducción en el mercado de sistemas de inteligencia artificial de alto riesgo específicos.

En caso de infracción, los requisitos permitirán a las autoridades nacionales acceder a la información necesaria para investigar si el uso de la inteligencia artificial cumplía la legislación.

¿Qué papel tendrá la normalización en el Reglamento de Inteligencia Artificial?

En virtud del Reglamento de Inteligencia Artificial, los sistemas de inteligencia artificial de alto riesgo estarán sujetos a requisitos específicos. Las normas armonizadas europeas desempeñarán un papel clave en la aplicación de esos requisitos.

En mayo de 2023, la Comisión Europea encargó a las organizaciones europeas de normalización CEN y CENELEC que elaboraran normas sobre esos requisitos de alto riesgo. Este mandato se va a modificar para adaptarlo al texto final del Reglamento de Inteligencia Artificial.

Las organizaciones europeas de normalización tendrán hasta finales de abril de 2025 para elaborar y publicar las normas. A continuación, la Comisión evaluará y posiblemente aprobará esas normas, que se publicarán en el *Diario Oficial de la Unión Europea*. Una vez publicadas, estas normas otorgarán una «presunción de conformidad» a los sistemas de inteligencia artificial programados con arreglo a ellas.

¿Cómo se regulan los modelos de inteligencia artificial de uso general?

Los **modelos de inteligencia artificial de uso general**, incluidos los grandes **modelos generativos de inteligencia artificial**, pueden servir para diversas tareas. Los distintos modelos pueden integrarse en un gran número de sistemas de inteligencia artificial.

Es crucial que cualquier proveedor de un sistema de inteligencia artificial que integre un modelo de inteligencia artificial de uso general disponga de toda la información necesaria para velar por que su sistema sea seguro y conforme con el Reglamento de Inteligencia Artificial.

Por lo tanto, el Reglamento de Inteligencia Artificial obliga a los proveedores de tales modelos a **divulgar determinada información a los proveedores de sistemas en fases posteriores**. Esta **transparencia** facilita una mejor comprensión de esos modelos.

Además, los proveedores de modelos deben dotarse de políticas que garanticen su respeto de la **legislación en materia de derechos de autor** a la hora de entrenar sus modelos.

Por otra parte, algunos de estos modelos podrían entrañar **riesgos sistémicos**, porque tienen gran capacidad o son objeto de un uso generalizado.

En la actualidad, se considera que los modelos de inteligencia artificial de uso general que hayan sido entrenados utilizando **una potencia informática total de más de 10^{25} operaciones de coma flotante por segundo** (FLOPS, por sus siglas en inglés) entrañan riesgos sistémicos. La Comisión podría actualizar o complementar este umbral a la luz de los avances tecnológicos y, además, en casos concretos, designar otros modelos según criterios suplementarios (por ejemplo, el número de usuarios o el grado de autonomía del modelo).

Los proveedores de modelos con riesgos sistémicos tienen la obligación de **evaluar y mitigar los riesgos, notificar los incidentes graves, llevar a cabo pruebas y evaluaciones avanzadas de los modelos** y garantizar la **ciberseguridad** de estos.

Se invita a los proveedores a colaborar con la Oficina Europea de Inteligencia Artificial y otras partes interesadas para elaborar un código de prácticas en el que se detallen las normas y, de este modo, se garantice el desarrollo seguro y responsable de sus modelos. Este código debe representar una herramienta central para que los proveedores de modelos de inteligencia artificial de uso general demuestren su cumplimiento.

¿Por qué el umbral adecuado para los sistemas de inteligencia artificial de uso general con riesgos sistémicos es de 10^{25} FLOPS?

Las FLOPS son un primer indicador de las capacidades de los modelos, y la Oficina Europea de Inteligencia Artificial puede actualizar al alza o a la baja el umbral exacto de FLOPS, por ejemplo, a la

luz de los avances en la medición objetiva de las capacidades de los modelos y de la evolución de la potencia informática necesaria para un determinado nivel de rendimiento.

Las capacidades de los modelos por encima de este umbral todavía no se comprenden en grado suficiente. Estos podrían plantear riesgos sistémicos, por lo que es razonable someter a sus proveedores al conjunto adicional de obligaciones.

¿Cuáles son las obligaciones relativas al mercado de agua y el etiquetado de la información de salida de inteligencia artificial establecidas en el Reglamento de Inteligencia Artificial?

El Reglamento de Inteligencia Artificial establece normas de transparencia sobre los contenidos producidos por la inteligencia artificial generativa a fin de hacer frente a los riesgos de manipulación, engaño y desinformación.

Obliga a los proveedores de sistemas de inteligencia artificial generativa a marcar la información de salida de la inteligencia artificial en un formato legible por máquina y a garantizar que sean detectables como generados o manipulados artificialmente. Las soluciones técnicas deben ser eficaces, interoperables, sólidas y fidedignas en la medida en que sea técnicamente viable, teniendo en cuenta las características específicas y las limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes.

Además, los usuarios de sistemas de inteligencia artificial generativa que generen o manipulen contenidos de imagen, audio o vídeo que constituyan ultrafalsificaciones deben revelar visiblemente que el contenido se ha generado o manipulado artificialmente. Los usuarios de un sistema de inteligencia artificial que genere o manipule texto que se publique con el fin de informar a la población sobre asuntos de interés público también deben divulgar que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el contenido generado mediante inteligencia artificial haya sido sometido a un proceso de revisión humana o control editorial y cuando una persona física o jurídica sea responsable editorial de la publicación del contenido.

La Oficina Europea de Inteligencia Artificial publicará directrices para aportar orientaciones adicionales a los proveedores y usuarios sobre las obligaciones establecidas en el artículo 50, que serán aplicables dos años después de la entrada en vigor del Reglamento de Inteligencia Artificial (el 2 de agosto de 2026).

La Oficina Europea de Inteligencia Artificial fomentará y facilitará la elaboración de códigos de prácticas a escala de la Unión para facilitar la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados de manera artificial.

¿Está preparado el Reglamento de Inteligencia Artificial para el futuro?

El Reglamento de Inteligencia Artificial establece un marco jurídico que responde a los nuevos avances, además de ser fácil y rápido de adaptar, y contempla una evaluación frecuente.

El Reglamento de Inteligencia Artificial establece obligaciones y requisitos vinculados a los resultados, pero confía las soluciones técnicas concretas y la puesta en funcionamiento principalmente a unas normas y códigos de prácticas impulsados por el sector que sean flexibles, a fin de adaptarse a los diferentes casos de uso y de facilitar nuevas soluciones tecnológicas.

Además, la propia legislación puede modificarse mediante actos delegados y de ejecución, por ejemplo para revisar la lista de casos de uso de alto riesgo del anexo III.

Por último, se llevarán a cabo evaluaciones frecuentes de determinadas partes del Reglamento de Inteligencia Artificial y, en última instancia, de todo el Reglamento, de manera que se podrá determinar cualquier necesidad de revisión y modificación.

¿Cómo regula el Reglamento de Inteligencia Artificial la identificación biométrica?

Queda prohibido el uso de la **identificación biométrica remota en tiempo real en lugares de acceso público** (es decir, el reconocimiento facial mediante circuito cerrado de televisión) con fines policiales. Los Estados miembros pueden introducir excepciones por ley que permitan el uso de la identificación biométrica remota en tiempo real en los casos siguientes:

- actividades policiales relacionadas con dieciséis delitos concretos muy graves;
- búsqueda selectiva de víctimas específicas, secuestros, trata y explotación sexual de seres

humanos y personas desaparecidas, o

- o prevención de amenazas para la vida o la seguridad física de las personas o respuesta a la amenaza actual o previsible de un ataque terrorista.

Cualquier uso excepcional estará sujeto a la **autorización previa de una autoridad judicial o administrativa independiente**, cuya decisión será vinculante. En caso de urgencia, la aprobación podrá concederse en un plazo de 24 horas; si se rechaza la autorización, deberán suprimirse todos los datos y el resultado.

Habrà de ir precedida de una **evaluación previa de las repercusiones desde el punto de vista de los derechos fundamentales** y debe **notificarse a la autoridad de vigilancia del mercado pertinente y a la autoridad de protección de datos**. En caso de urgencia, la utilización del sistema podrá iniciarse sin el registro.

El uso de sistemas de inteligencia artificial para la **identificación biométrica remota posterior** (identificación de personas en material de vídeo recogido previamente) de personas investigadas requiere la **autorización previa** de una autoridad judicial o de una autoridad administrativa independiente, y la notificación a la autoridad de protección de datos y vigilancia del mercado.

¿Por qué son necesarias normas específicas sobre la identificación biométrica remota?

La identificación biométrica puede adoptar distintas formas. La autenticación y verificación biométricas, es decir, el desbloqueo de un teléfono inteligente o la verificación o autenticación en los pasos fronterizos para comprobar la identidad de una persona mediante el cotejo de sus documentos de viaje (correspondencia uno a uno) siguen sin estar reguladas, ya que no suponen un grave riesgo para los derechos fundamentales.

Por el contrario, la identificación biométrica también puede utilizarse a distancia, por ejemplo, para identificar a personas en una multitud, lo que puede afectar gravemente a la privacidad en el espacio público.

La precisión de los sistemas de reconocimiento facial puede variar considerablemente en función de factores muy diversos, tales como la calidad de la cámara, la luz, la distancia, la base de datos, el algoritmo y la etnia, edad o sexo del sujeto. Lo mismo se aplica a los sistemas de reconocimiento vocal y de la forma de andar y otros sistemas biométricos. Estos avanzados sistemas están reduciendo sin cesar sus tasas de falsa aceptación.

Si bien un índice de precisión del 99 % puede parecer bueno en general, supone un riesgo considerable cuando el resultado lleve a sospechar de una persona inocente. Incluso una tasa de error del 0,1 % puede tener efectos graves cuando se aplica a grandes poblaciones, por ejemplo, en las estaciones de tren.

¿Cómo protegen las normas los derechos fundamentales?

Ya existe una sólida protección de los derechos fundamentales y la no discriminación a escala de la UE y de los Estados miembros, pero la complejidad y la opacidad de determinadas aplicaciones de inteligencia artificial («cajas negras») pueden plantear problemas.

Todo planteamiento de la inteligencia artificial centrado en el ser humano supone velar por que las aplicaciones de inteligencia artificial cumplan la legislación en materia de derechos fundamentales. Mediante la integración de los requisitos de rendición de cuentas y transparencia en la programación de los sistemas de inteligencia artificial de alto riesgo y la mejora de las capacidades de ejecución, podemos garantizar que estos sistemas se diseñen teniendo en cuenta desde el principio el cumplimiento de la ley. En caso de infracción, esos requisitos permitirán a las autoridades nacionales acceder a la información necesaria para investigar si el uso de la inteligencia artificial se ajusta al Derecho de la UE.

Además, el Reglamento de Inteligencia Artificial exige que determinados usuarios de sistemas de inteligencia artificial de alto riesgo lleven a cabo una evaluación de impacto en relación con los derechos fundamentales.

¿Qué es una evaluación de impacto en los derechos fundamentales? ¿Quién debe llevar a cabo tal evaluación y cuándo?

Los proveedores de sistemas de inteligencia artificial de alto riesgo deben llevar a cabo una evaluación de riesgos y diseñar el sistema de manera que se minimicen esos riesgos para la salud, la seguridad y los derechos fundamentales.

Sin embargo, algunos riesgos para los derechos fundamentales solo pueden detectarse completamente teniendo en cuenta el contexto de uso del sistema de inteligencia artificial de alto riesgo. Cuando se utilicen sistemas de inteligencia artificial de alto riesgo en ámbitos especialmente sensibles de posible asimetría de poder, es necesario tener en cuenta esos riesgos adicionales.

Por consiguiente, los usuarios que sean organismos de Derecho público o agentes privados que presten servicios públicos, así como los operadores que suministren sistemas de inteligencia artificial de alto riesgo que realicen evaluaciones de la solvencia crediticia o evaluaciones de precios y de riesgos en los seguros de salud y de vida, deberán llevar a cabo una evaluación de las repercusiones en los derechos fundamentales y notificar los resultados a la autoridad nacional.

En la práctica, muchos usuarios también tendrán que llevar a cabo una evaluación de impacto relativa a la protección de datos. Para evitar solapamientos sustanciales en tales casos, la evaluación de impacto sobre los derechos fundamentales se llevará a cabo junto con esa evaluación de impacto relativa a la protección de datos.

¿Cómo hace frente este Reglamento a los sesgos raciales y de género en la inteligencia artificial?

Es muy importante hacer hincapié en que los sistemas de inteligencia artificial **no creen ni reproduzcan sesgos**. Al contrario, si se diseñan y utilizan adecuadamente, los **sistemas de inteligencia artificial pueden contribuir a reducir los prejuicios y la discriminación estructural existentes** y, por lo tanto, facilitar la adopción de decisiones más equitativas y no discriminatorias (por ejemplo, en la contratación de personal).

Los **nuevos requisitos obligatorios aplicables a todos los sistemas de inteligencia artificial de alto riesgo servirán a tal fin**. Los sistemas de inteligencia artificial deben ser **técnicamente sólidos** para garantizar que se ajusten a su finalidad y no produzcan resultados sesgados, tales como falsos positivos o negativos, que afecten de manera desproporcionada a los grupos marginados, por ejemplo, aquellos definidos por el origen racial o étnico, el sexo, la edad y otras características protegidas.

Los sistemas de alto riesgo tendrán que **entrenarse y ensayarse con conjuntos de datos lo suficientemente representativos** como para **reducir al mínimo el riesgo de incorporación de sesgos injustos** al modelo y asegurar que tales situaciones puedan solventarse mediante las medidas apropiadas de detección y corrección de sesgos y otras medidas paliativas.

También deberán poder **rastrearse y auditarse**, garantizando la **conservación de la documentación** pertinente, incluidos los datos utilizados para entrenar el algoritmo, algo que es clave en las investigaciones *a posteriori*.

El **sistema de cumplimiento antes y después de su comercialización** ha de garantizar que estos sistemas sean objeto de un **seguimiento periódico** y que se **neutralicen rápidamente los riesgos potenciales**.

¿Cuándo será plenamente aplicable el Reglamento de Inteligencia Artificial?

El Reglamento de Inteligencia Artificial se aplicará dos años después de su entrada en vigor el 2 de agosto de 2026, con excepción de las disposiciones específicas siguientes:

- las prohibiciones, definiciones y disposiciones relacionadas con la alfabetización en materia de inteligencia artificial se aplicarán seis meses después de su entrada en vigor el 2 de febrero de 2025;
- las normas sobre gobernanza y las obligaciones relativas a la inteligencia artificial de uso general será aplicables doce meses después de su entrada en vigor el 2 de agosto de 2025;
- las obligaciones de los sistemas de inteligencia artificial de alto riesgo clasificados como de alto riesgo por estar integrados en productos regulados que figuren en el anexo II (lista de legislación de armonización de la Unión), se aplicarán 36 meses después de su entrada en vigor el 2 de agosto de 2027.

¿Cómo se hará cumplir el Reglamento de Inteligencia Artificial?

El Reglamento de Inteligencia Artificial establece un sistema de gobernanza de dos niveles, por el que las **autoridades nacionales** son responsables de supervisar y hacer cumplir las normas relativas a los sistemas de inteligencia artificial, mientras que la UE lo es de regular los modelos de inteligencia artificial de uso general.

Para garantizar la coherencia y la cooperación a escala de la UE, se creará el **Comité Europeo de Inteligencia Artificial**, compuesto por representantes de los Estados miembros, con subgrupos

especializados para los reguladores nacionales y otras autoridades competentes.

La **Oficina Europea de Inteligencia Artificial**, que es el organismo de ejecución del Reglamento de Inteligencia Artificial de la Comisión, aportará orientaciones estratégicas al Comité Europeo de Inteligencia Artificial.

Además, el Reglamento de Inteligencia Artificial establece dos órganos consultivos para las observaciones de los expertos: la **Comisión Técnica Científica** y el **Foro Consultivo**. Estos organismos ofrecerán valiosas observaciones de las partes interesadas y de las comunidades científicas interdisciplinarias, que servirán de base para la toma de decisiones y garantizarán un planteamiento equilibrado en materia de fomento de la inteligencia artificial.

¿Por qué se necesita un Comité Europeo de Inteligencia Artificial y cuál será su cometido?

El Comité Europeo de Inteligencia Artificial estará formado por **representantes de alto nivel de las autoridades nacionales de supervisión competentes** y el Supervisor Europeo de Protección de Datos. Como asesor clave, este Comité aporta orientaciones sobre todas las cuestiones relacionadas con la política en la materia, y en particular la regulación de la inteligencia artificial, la política de innovación y excelencia y la cooperación internacional sobre inteligencia artificial.

El Comité Europeo de Inteligencia Artificial desempeña un papel crucial a la hora de garantizar una aplicación fluida, eficaz y armonizada del Reglamento de Inteligencia Artificial. Este Comité servirá de foro en el que los reguladores de la inteligencia artificial, esto es, la Oficina Europea de Inteligencia Artificial, las autoridades nacionales y el Supervisor Europeo de Protección de Datos, puedan coordinar la aplicación coherente del Reglamento de Inteligencia Artificial.

¿Cuáles son las sanciones por las infracciones?

Los Estados miembros tendrán que establecer sanciones efectivas, proporcionadas y disuasorias por las infracciones de las normas aplicables a los sistemas de inteligencia artificial.

El Reglamento fija umbrales que deberán tenerse en cuenta:

- o **hasta 35 millones de euros o el 7 %** del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, si este importe fuera superior, por las infracciones por **incumplimiento o prácticas prohibidas** en relación con los requisitos sobre los datos;
- o **hasta 15 millones de euros o el 3 %** del volumen de negocios anual total a escala mundial del ejercicio financiero anterior **por el incumplimiento de cualquier otro requisito** u obligación del Reglamento;
- o **hasta 7,5 millones de euros o el 1,5 %** del volumen de negocios total anual a escala mundial del ejercicio anterior por el **suministro de información incorrecta, incompleta o engañosa** a los organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud;
- o en cada categoría de infracción, el umbral sería el menor de los dos importes para las pymes y el más elevado para las demás empresas.

La Comisión también puede hacer cumplir las normas sobre los proveedores de modelos de inteligencia artificial de uso general mediante multas, teniendo en cuenta el umbral siguiente:

- o **hasta 15 millones de euros o el 3 %** del volumen de negocios anual total a escala mundial del ejercicio financiero anterior **por el incumplimiento de cualquier obligación** o medidas exigidas por la Comisión en virtud del Reglamento;

Como se supone que las instituciones, agencias y organismos de la UE deben dar ejemplo, también estarán sujetas a las normas y a las posibles sanciones. El Supervisor Europeo de Protección de Datos estará facultado para imponerles multas en caso de incumplimiento.

¿Cómo se redactará el código de prácticas de la inteligencia artificial de uso general?

La elaboración del primer código sigue un proceso inclusivo y transparente. Se establecerá un pleno del código de prácticas para facilitar el proceso de redacción iterativa, compuesto por todos los proveedores de modelos de inteligencia artificial de uso general interesados y admisibles, los proveedores posteriores que integren un modelo de inteligencia artificial de uso general en su sistema de inteligencia artificial, otras organizaciones del sector y otras organizaciones de partes interesadas como la sociedad civil o las organizaciones de titulares de derechos, además de expertos del mundo académico y otros expertos independientes.

La Oficina Europea de Inteligencia Artificial ha abierto una convocatoria de manifestaciones de interés para participar en la elaboración del primer código de prácticas. Paralelamente a esta convocatoria de manifestaciones de interés, se va a poner en marcha una consulta multilateral para recabar opiniones y observaciones de todas las partes interesadas sobre el primer código de prácticas. La primera redacción de ese código se basará en las respuestas y observaciones. El código aprovechará desde el principio puntos de vista y conocimientos técnicos diversos.

El pleno se dividirá en cuatro grupos de trabajo, a fin de facilitar los debates centrados en temas concretos pertinentes para especificar las obligaciones de los proveedores de modelos de inteligencia artificial de uso general y modelos de inteligencia artificial de uso general con riesgo sistémico. Los participantes en el pleno serán libres de elegir uno o más grupos de trabajo en los que deseen participar. Las reuniones se celebrarán exclusivamente en línea.

La Oficina Europea de Inteligencia Artificial designará presidentes y, en su caso, vicepresidentes para cada uno de los cuatro grupos de trabajo del pleno, seleccionados de entre los expertos independientes interesados. Los presidentes resumirán las observaciones y los comentarios de los participantes en el pleno para redactar iterativamente el primer código de prácticas.

Como principales destinatarios del código, se invitará a los proveedores de modelos de inteligencia artificial de uso general a talleres específicos para que contribuyan a dar forma a cada ronda de redacción iterativa, además de participar en el pleno.

Transcurridos nueve meses, la versión final del primer código de prácticas se presentará en un pleno de clausura, cuya celebración está prevista en abril, y luego se publicará. El pleno de clausura ofrecerá a los proveedores de modelos de inteligencia artificial de uso general la oportunidad de manifestar si tienen previsto utilizar el código.

En caso de aprobarse, ¿cómo servirá el código de prácticas a los proveedores de modelos de inteligencia artificial de uso general como herramienta central para el cumplimiento?

Al final del proceso de elaboración del código de prácticas, la Oficina Europea de Inteligencia Artificial y el Comité Europeo de Inteligencia Artificial evaluarán la adecuación del código y publicarán su evaluación. Tras esta última, la Comisión podrá decidir aprobar el código de prácticas y conferirle validez general dentro de la Unión mediante actos de ejecución. Si la Oficina Europea de Inteligencia Artificial no considerara idóneo el código de prácticas al entrar en vigor el Reglamento, la Comisión podría establecer normas comunes a efectos del cumplimiento de las obligaciones pertinentes.

Por lo tanto, los proveedores de modelos de inteligencia artificial de uso general pueden basarse en el código de prácticas para demostrar el cumplimiento de las obligaciones establecidas en el Reglamento de Inteligencia Artificial.

Con arreglo a este Reglamento, el código de prácticas debe comprender objetivos, medidas y, en su caso, indicadores clave de rendimiento (ICR).

Los proveedores que se adhieran al código deberán informar periódicamente a la Oficina Europea de Inteligencia Artificial sobre el cumplimiento de las medidas adoptadas y sus resultados, también medidos con respecto a los indicadores clave de rendimiento, según proceda.

Esto facilitará las labores de ejecución de la Oficina Europea de Inteligencia Artificial, sobre la base de las competencias conferidas a la Comisión por el Reglamento de Inteligencia Artificial. Esto abarcará la capacidad de llevar a cabo evaluaciones de modelos de inteligencia artificial de uso general, solicitar información y medidas a los proveedores de modelos y aplicar sanciones.

La Oficina Europea de Inteligencia Artificial fomentará y facilitará, según proceda, la revisión y la adaptación del código, de manera que este recoja los avances en la tecnología y el estado de la técnica.

Una vez que se haya publicado una norma armonizada y que la Oficina Europea de Inteligencia Artificial la considere idónea a la hora de cubrir las obligaciones pertinentes, el cumplimiento de una norma armonizada europea deberá ofrecer a los proveedores la presunción de conformidad.

Además, los proveedores de modelos de inteligencia artificial de uso general deberán poder demostrar el cumplimiento utilizando medios alternativos adecuados si no hay códigos de prácticas o normas armonizadas, o si han decidido no basarse en ellos.

¿Contiene el Reglamento de Inteligencia Artificial disposiciones relativas a la protección del medio ambiente y la sostenibilidad?

El objetivo de la propuesta sobre la inteligencia artificial es afrontar los riesgos para la seguridad y

los derechos fundamentales, incluido el derecho fundamental a un alto grado de protección medioambiental. El medio ambiente es también uno de los intereses jurídicos expresamente mencionados y protegidos.

Se pide a la Comisión que solicite a las organizaciones europeas de normalización que elaboren un documento de normalización sobre los procesos de notificación y documentación para mejorar el rendimiento de los sistemas de inteligencia artificial en cuanto a su uso de recursos, por ejemplo, sobre la reducción del consumo de energía y otros recursos por parte del sistema de inteligencia artificial de alto riesgo durante su ciclo de vida, y sobre la creación eficiente desde el punto de vista energético de modelos de inteligencia artificial de uso general.

Además, a más tardar dos años después de la fecha de aplicación del Reglamento y, posteriormente, cada cuatro años, se pide a la Comisión que presente un informe sobre la revisión de los avances en la elaboración de los documentos de normalización sobre la creación eficiente desde el punto de vista energético de modelos de uso general y que estudie la necesidad de nuevas medidas o acciones, incluso con carácter vinculante.

Además, los proveedores de modelos de inteligencia artificial de uso general, que se entrenen con grandes cantidades de datos y, en consecuencia, tiendan a consumir mucha energía, estarán obligados a divulgar ese consumo. En el caso de los modelos de inteligencia artificial de uso general con riesgos sistémicos, también deberá evaluarse la eficiencia energética.

La Comisión está facultada para elaborar un método de medición adecuado y comparable para estas obligaciones de divulgación.

¿Cómo podrán apoyar la innovación las nuevas normas?

La normativa podrá mejorar la aceptación de la inteligencia artificial de dos maneras. Por una parte, la mayor confianza de los usuarios aumentará la demanda de inteligencia artificial utilizada por las empresas y las autoridades públicas. Por otra parte, al mejorar la seguridad jurídica y armonizarse las normas, los proveedores de inteligencia artificial accederán a mercados más grandes, con productos que los usuarios y consumidores apreciarán y adquirirán. Las normas solo se aplicarán cuando sea estrictamente necesario y de manera que se reduzca al mínimo la carga para los agentes económicos, con una estructura de gobernanza ligera.

El Reglamento de Inteligencia Artificial permite, además, la creación de **espacios controlados de pruebas y ensayo en condiciones reales**, que aportan un entorno controlado para probar tecnologías innovadoras durante un tiempo limitado, fomentando así la innovación por parte de las empresas, las pymes y las empresas emergentes de conformidad con el Reglamento de Inteligencia Artificial. Estas y otras medidas como las nuevas **redes de centros de excelencia en inteligencia artificial**, la **asociación público-privada sobre inteligencia artificial, datos y robótica**, y el acceso a los **centros de innovación digital** y las **instalaciones de ensayo y experimentación de inteligencia artificial** contribuirán a crear las condiciones generales adecuadas para que las empresas programen y usen inteligencia artificial.

Los ensayos en el mundo real de los sistemas de inteligencia artificial de alto riesgo pueden llevarse a cabo durante un máximo de seis meses, plazo que podrá prorrogarse otros seis meses. Antes de los ensayos, se elaborará un plan que se presentará a la autoridad de vigilancia del mercado, la cual deberá aprobarlo junto con las condiciones de ensayo concretas, considerándose, si no se ha dado respuesta en un plazo de treinta días, que el silencio administrativo es positivo. Los ensayos podrán ser objeto de inspecciones sin previo aviso por parte de la autoridad.

Los ensayos en el mundo real solo podrán llevarse a cabo con salvaguardias específicas; por ejemplo, los usuarios de los sistemas sometidos a tales ensayos tendrán que dar su consentimiento informado, los ensayos no deberán tener ningún efecto negativo en ellos, los resultados deberán ser reversibles o desechables, y sus datos se suprimirán una vez finalizada la prueba. Deberá ofrecerse una protección especial a los grupos que sean vulnerables, por ejemplo, debido a su edad o discapacidad física o mental.

¿Qué papel desempeña el Pacto sobre la Inteligencia Artificial en la aplicación del Reglamento de Inteligencia Artificial?

El Pacto sobre la Inteligencia Artificial, puesto en marcha por el comisario Breton en mayo de 2023, tiene por objeto intensificar los contactos entre la Oficina Europea de Inteligencia Artificial y las organizaciones en la materia (primer pilar) y fomentar el compromiso voluntario del sector de empezar a cumplir los requisitos del Reglamento de Inteligencia Artificial antes del plazo legal (segundo pilar).

En concreto, en el marco del primer pilar, los participantes contribuirán a la creación de una

comunidad colaborativa, mediante el intercambio de experiencias y conocimientos. Esto abarcará talleres organizados por la Oficina Europea de Inteligencia Artificial para facilitar a los participantes una mejor comprensión del Reglamento de Inteligencia Artificial, sus responsabilidades y la manera de prepararse para su cumplimiento. A su vez, la Oficina Europea de Inteligencia Artificial podrá recabar información sobre las mejores prácticas y las dificultades de los participantes.

En el marco del segundo pilar, se anima a las organizaciones a divulgar dinámicamente los procesos y prácticas que estén aplicando para adelantar el cumplimiento, mediante compromisos voluntarios. Estos se conciben como «declaraciones de compromiso» y contemplarán acciones (previstas o en curso) para cumplir algunos de los requisitos del Reglamento de Inteligencia Artificial.

La mayoría de las normas del Reglamento de Inteligencia Artificial (por ejemplo, algunos requisitos sobre los sistemas de inteligencia artificial de alto riesgo) se aplicarán al final de un período transitorio (es decir, el período comprendido entre la entrada en vigor y la fecha de aplicabilidad).

A este respecto, y en el marco del Pacto sobre la Inteligencia Artificial, la Oficina Europea de Inteligencia Artificial pide a todas las organizaciones que se adelanten y cumplan ya algunas de las disposiciones fundamentales del Reglamento de Inteligencia Artificial, a fin de mitigar los riesgos para la salud, la seguridad y los derechos fundamentales lo antes posible.

Más de 700 organizaciones ya han manifestado su interés por adherirse a la iniciativa del Pacto sobre la Inteligencia Artificial, a raíz de una convocatoria abierta en noviembre de 2023. El 6 de mayo se celebró una primera sesión informativa en línea, con 300 participantes. La firma oficial de los compromisos voluntarios está prevista en el otoño de 2024. En la primera semana de septiembre se celebrará un taller centrado en el Pacto sobre la Inteligencia Artificial.

¿Cuál es la dimensión internacional del planteamiento adoptado por la UE?

La inteligencia artificial tiene consecuencias y retos que superan las fronteras, por lo cual es importante la cooperación internacional. La Oficina Europea de Inteligencia Artificial es responsable de las relaciones internacionales de la Unión Europea en el ámbito de la inteligencia artificial, sobre la base del Reglamento de Inteligencia Artificial y del Plan Coordinado sobre la Inteligencia Artificial. La UE intenta promover la gestión responsable y la buena gobernanza de la inteligencia artificial en colaboración con sus socios internacionales y en consonancia con el sistema multilateral basado en normas y los valores que defiende.

La UE se compromete bilateral y multilateralmente a promover una inteligencia artificial fiable, ética y centrada en el ser humano. En consecuencia, la UE participa en foros multilaterales en los que se debate la inteligencia artificial, concretamente el G7, el G20, la OCDE, el Consejo de Europa, la Alianza Mundial sobre la Inteligencia Artificial y las Naciones Unidas. También mantiene estrechos contactos bilaterales, por ejemplo, con Canadá, los Estados Unidos, la India, Japón, Corea del Sur, Singapur y la región de América Latina y el Caribe.

**Actualizado el 1.8.2024.*

QANDA/21/1683

Personas de contacto para la prensa:

[Thomas Regnier](#) (+32 2 29 9 1099)

[Patricia Poropat](#) (+32 2 298 04 85)

Solicitudes del público en general: [Europe Direct](#) por teléfono [00 800 67 89 10 11](#) , o por [e-mail](#)