COMISIÓN EUROPEA

UBA #1 Iberoamérica ranking QS

IALAB

Propuesta de Reglamento sobre un enfoque europeo de la Inteligencia Artificial

21 de abril de 2021

Esta infografía realizada desde UBA-IALAB refleja los principales aspectos del Reglamento Europeo de IA, que busca convertir a Europa en el centro mundial de la IA fiable. Para ello, clasifica a los sistemas de IA siguiendo un enfoque basado en el riesgo, señala prohibiciones y establece requisitos obligatorios para su uso

Objetivos de la propuesta

1. Garantizar sistemas de IA seguros, que respeten la legislación vigente sobre derechos fundamentales y valores de la Unión Europea

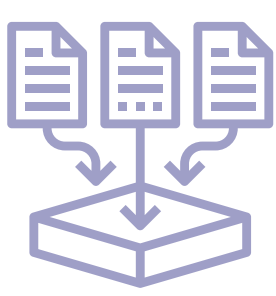
2. Garantizar la seguridad jurídica para facilitar la inversión y la innovación en IA

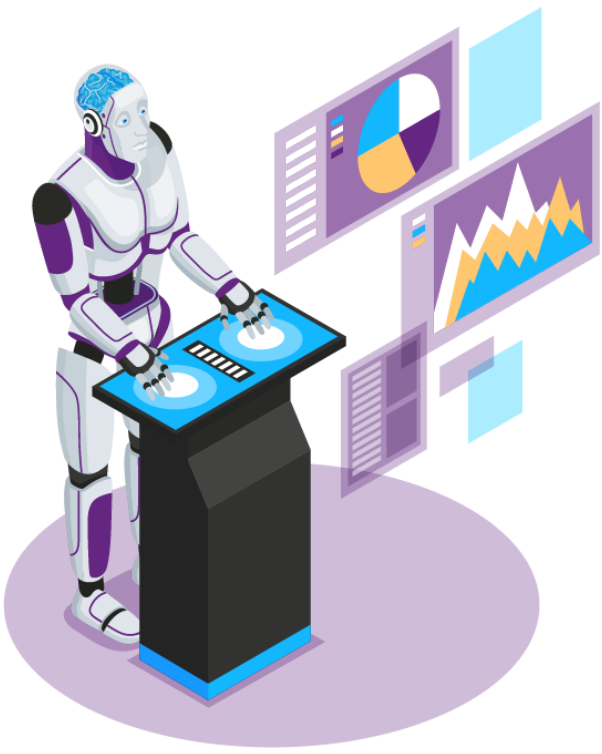
3. Mejorar la gobernanza y la aplicación de la ley existente y requisitos de seguridad aplicables a los sistemas de IA

4. Facilitar el desarrollo de un mercado único para aplicaciones de IA legales, seguras y confiables y prevenir la fragmentación del mercado

Propuestas para lograr los objetivos

Enfoque regulatorio horizontal, equilibrado y basado en el riesgo, sin crear restricciones al comercio





Marco legal, sólido y flexible orientado hacia el futuro. Permitir la adaptación dinámica frente a la evolución tecnológica

Prohibiciones de prácticas de IA por ser contrarias a valores de la unión

Reparación eficaz en caso de infracciones a derechos fundamentales

Restricciones a usos de sistemas para la identificación biométrica remota con fines policiales

Establece requisitos que deben cumplir los sistemas de IA

Procedimientos de evaluación ex ante y ex post (supervisión humana)

Obligaciones a proveedores/as y usuarios/as para garantizar la seguridad y respeto de derechos los fundamentales durante todo el ciclo de vida de los sistemas de IA

Minimizar el riesgo de decisiones erróneas o sesgadas asistidas por IA

¿Qué es un sistema de inteligencia artificial?

Software que puede generar resultados como contenido, predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales

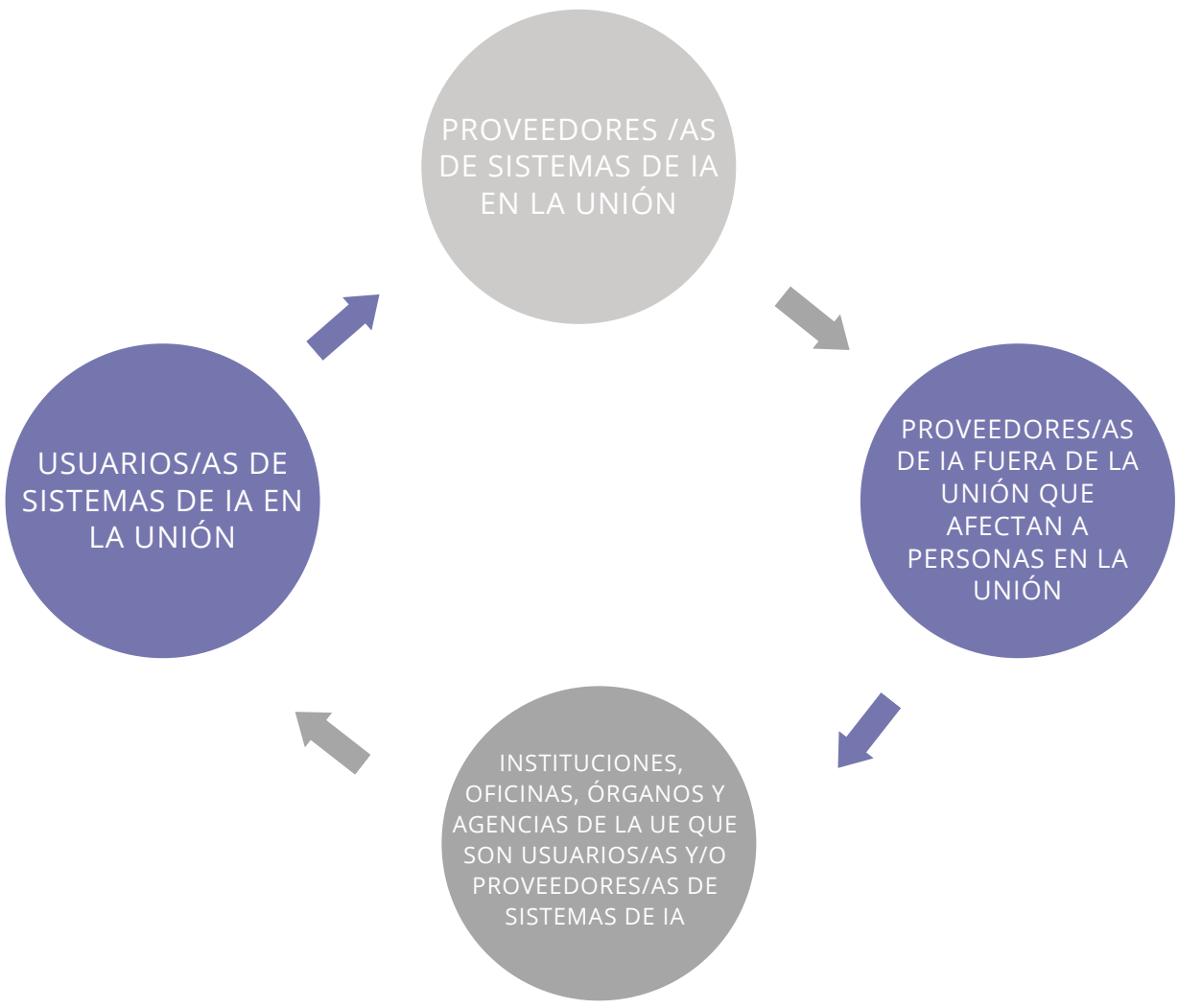
Son diseñados para funcionar con distintos niveles de autonomía; automatizar parcial o totalmente ciertas actividades (servicios, procesos, toma de decisiones o acciones)

Sistemas de identificación biométrica

Sistemas de IA de identificación a distancia de personas mediante la comparación de los datos biométricos de una persona con aquellos contenidos en una base de datos, sin conocimiento previo de si la persona está presente, independientemente de la tecnología, los procesos o los tipos de datos biométricos específicos utilizados. Su uso requiere autorización previa judicial o administrativa

Sistemas en tiempo real	La captura de los datos biométricos, la comparación y la identificación ocurren instantáneamente, casi instantáneamente o en cualquier caso sin un retraso significativo
Sistemas postales	Los datos biométricos ya se han capturado y la comparación e identificación se producen solo después de un retraso significativo

Sujetos alcanzados por el reglamento



Excepciones de aplicación del Reglamento

Sistemas de IA desarrollados o utilizados exclusivamente con fines militares

Autoridades públicas de un tercer país u organizaciones internacionales que utilicen sistemas de IA en el marco de acuerdos internacionales de cooperación policial y judicial con la Unión o con uno o más Estados miembros

Cuatro niveles de riesgo

Riesgo inaceptable

Alto riesgo

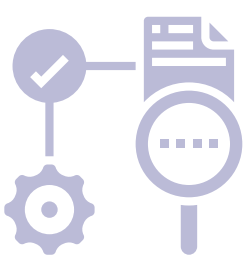
Riesgo limitado

Riesgo mínimo

1. Riesgo inaceptable

Prácticas prohibidas

Comercialización, puesta en servicio o uso de un sistema de IA que despliega técnicas subliminales más allá de la conciencia de una persona para distorsionar materialmente el comportamiento de una persona de modo que cause o pueda causarle a esa persona u otra un daño físico o psicológico



Puesta en el mercado, puesta en servicio o uso de un sistema de IA que explote cualquiera de las vulnerabilidades de un grupo de personas debido a su edad, discapacidad física o mental, con el fin de distorsionar materialmente el comportamiento de una persona de una manera que cause o pueda causar a esa persona u otra un daño físico o psicológico

Comercialización, puesta en servicio o uso de sistemas de IA por parte de las autoridades públicas o en su nombre, para la evaluación o clasificación de la confiabilidad de las personas durante un cierto período de tiempo, en función de su comportamiento social o personal, con la puntuación social que conduce a uno o ambos de los siguientes:

1. El trato perjudicial o desfavorable de determinadas personas o grupos, no relacionado con los contextos en que se generaron o recopilaron los datos originalmente

2. El trato perjudicial o desfavorable de determinadas personas o grupos injustificado o desproporcionado con su comportamiento social o su gravedad

Uso de sistemas de identificación biométrica remota 'en tiempo real' en espacios de acceso público con el propósito de hacer cumplir la ley, salvo que dicho uso sea estrictamente necesario para:

-la búsqueda de posibles víctimas de delitos;

-la prevención de una amenaza a la vida o seguridad física o de un ataque terrorista;

-la localización, identificación o enjuiciamiento de un autor o sospechoso de un delito penado con una pena privativa de libertad o una orden de internamiento por un período máximo de al menos tres años

2. Riesgo alto

Sistemas de IA permitidos sujetos al cumplimiento de requisitos y una evaluación de conformidad ex ante

1. Sistema de IA está destinado a ser utilizado como un componente de seguridad de un producto, o un producto en sí mismo

2. Producto cuyo componente de seguridad es el sistema de IA, o el propio sistema de IA como producto. Deben someterse a una evaluación de conformidad por parte de un tercero con vistas a la comercialización o puesta en servicio de ese producto

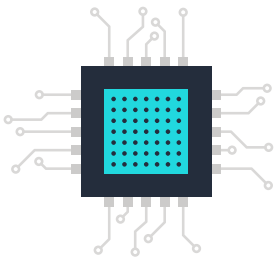
3. Sistemas de IA cuyos riesgos ya se han materializado o es probable que se materialicen en un futuro próximo

4. Sistemas de IA que suponen un riesgo de daño a la salud y seguridad o un riesgo de impacto adverso sobre los derechos fundamentales (gravedad y probabilidad de ocurrencia equivalente o mayor al riesgo de daño de los sistemas de IA de alto riesgo)

Incluye:

Infraestructuras críticas que podrían poner en riesgo la vida y la salud de los ciudadanos/as (por ejemplo: transporte)

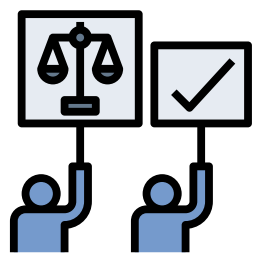
Formación educativa o vocacional que puede determinar el acceso a la educación y el curso profesional de la vida de alguien (por ejemplo: calificación de exámenes)



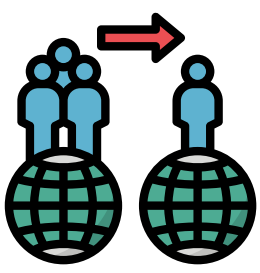
Componentes de seguridad de los productos (por ejemplo: aplicación de IA en cirugía asistida por robot)

Empleo, gestión y acceso al trabajo por cuenta propia (por ejemplo: software de clasificación de CV para los procedimientos de contratación)

Servicios públicos y privados esenciales (por ejemplo, calificación crediticia que niega a los ciudadanos la oportunidad de obtener un préstamo)



Aplicación de la ley que pueda interferir con los derechos fundamentales (por ejemplo: evaluación de la confiabilidad de las pruebas)

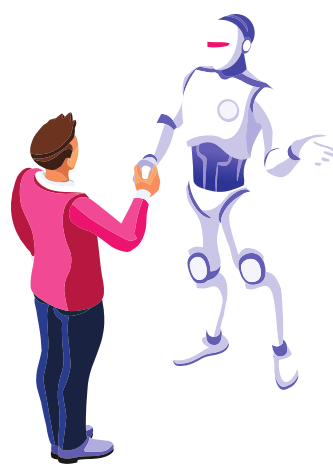


Gestión de migración, asilo y control de fronteras (por ejemplo: verificación de la autenticidad de los documentos de viaje)

Administración de justicia y procesos democráticos (por ejemplo: la aplicación de la ley a un conjunto concreto de hechos)

3. Riesgo limitado

Sistemas de IA con obligaciones específicas de transparencia (usuarios/as deben ser conscientes de que están interactuando con una máquina para poder tomar una decisión informada de continuar o dar un paso atrás)



4. Riesgo mínimo

Comprende la gran mayoría de los sistemas de IA. El Reglamento no resulta aplicable porque estos sistemas representan un riesgo mínimo o nulo para los derechos o la seguridad de los ciudadanos/as. Ej: videojuegos habilitados para IA o filtros de spam

Criterios para la determinación del riesgo

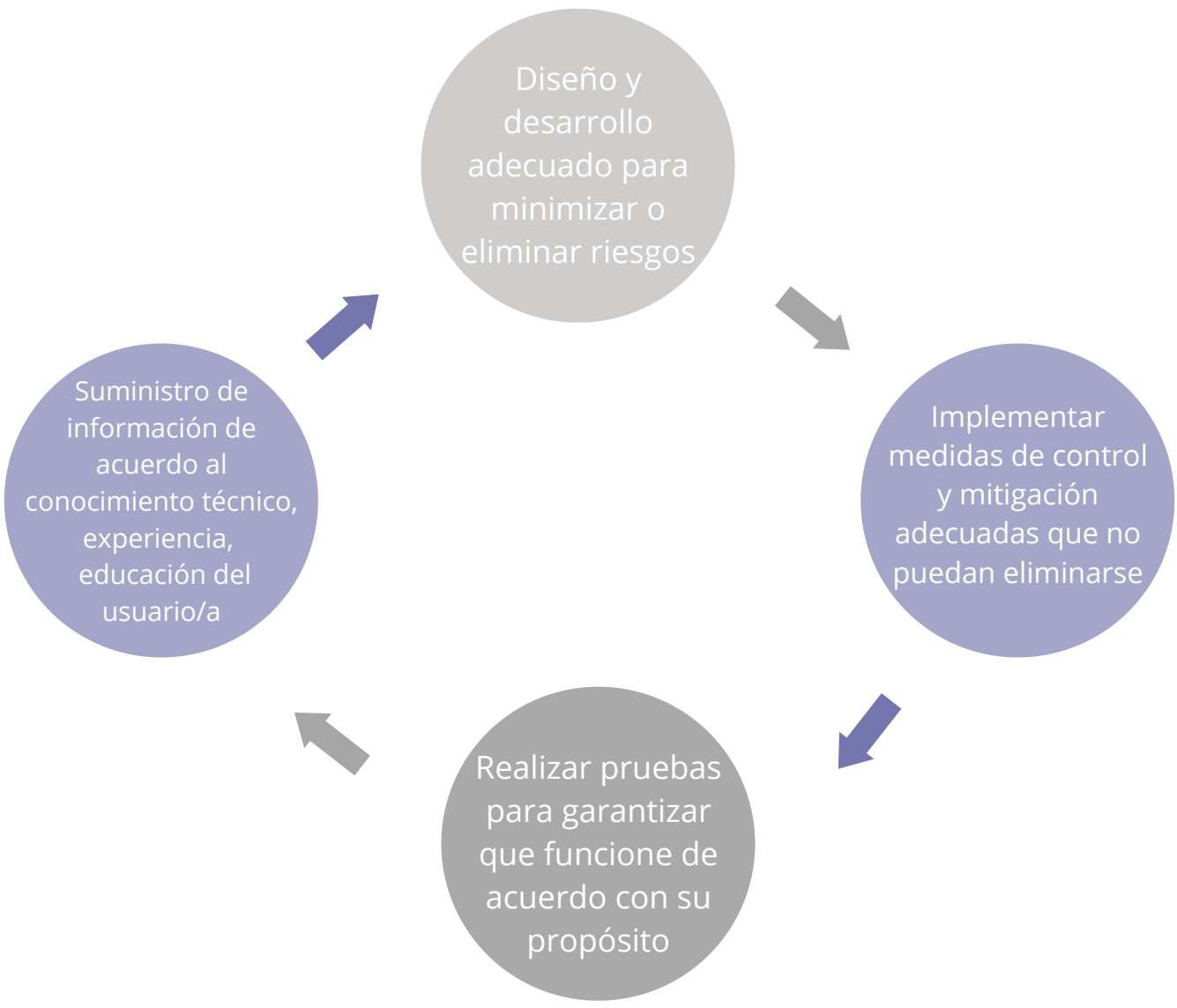
01	*Finalidad prevista del sistema de IA*
02	*Medida de utilización del sistema*
03	*Medida en que cause daños a la salud/seguridad*
04	*Alcance potencial del daño o impacto adverso a los derechos*
05	*Existencia de medidas efectivas de prevención, minimización o reparación*
06	*Posibilidad de revertir o excluir el resultado*
07	*Posición de vulnerabilidad o desequilibrio de la persona afectada*

Requisitos que deben cumplir los sistemas de IA de alto riesgo

1) Sistema de gestión del riesgo

- Presente durante todo el ciclo de vida como un proceso iterativo
- Identificación y análisis de los riesgos conocidos y previsibles
- Estimación y evaluación de riesgos al usuarlo y de otros riesgos que puedan surgir
- Adopción de medidas de gestión de riesgos

Medidas de gestión de riesgos



2) Conjuntos de datos de calidad

Prácticas adecuadas de gestión y gobernanza

Datos relevantes, representativos, libres de errores y completos, de acuerdo al propósito y entorno

Identificación de posibles lagunas o deficiencias de datos y cómo abordarlos

3) Documentación técnica

Sujeta a actualización constante

Demostrar que el sistema cumple con los requisitos

Previa a la comercialización o puesta en servicio del sistema

Proporcionar a las autoridades de supervisión la información necesaria

4) Mantenimiento de los registros

Los sistemas de IA de alto riesgo deben ser diseñados y desarrollados con capacidades que permitan el registro automático de eventos mientras se encuentran en funcionamiento. Deben ser capaces de:

1. Ajustarse a estándares reconocidos o especificaciones comunes
2. Garantizar un nivel de trazabilidad del sistema de IA a lo largo de su ciclo de vida apropiado al propósito del sistema

5) Transparencia y provisión de información

Funcionamiento transparente de los sistemas que permita a los usuarios/as interpretar la salida y utilizarla de forma adecuada

Incluir instrucciones de uso que incluya información concisa, completa, correcta y clara que sea relevante, accesible y comprensible para los usuarios/as acerca de:

1. Identidad y datos de contacto del proveedor/a o representante
2. Características, capacidades y limitaciones de rendimiento del sistema de IA
3. Especificaciones de los datos de entrada u otra información relevante
4. Cambios en el sistema de IA de alto riesgo y su desempeño, si los hubiere
5. Medidas de supervisión humana
6. Medidas técnicas para facilitar la interpretación de resultados; medidas de mantenimiento y cuidado para garantizar correcto funcionamiento

6) Supervisión humana

Durante todo el período en que el sistema de IA esté en uso

Objetivo: prevenir o minimizar riesgos para la salud, seguridad o los derechos fundamentales al utilizar sistemas de IA de alto riesgo, de acuerdo con su finalidad prevista o en condiciones de uso indebido razonablemente previsible

Medidas para garantizar la supervisión humana que permitan al usuario/a:

1. Comprender capacidades y limitaciones del sistema de IA y monitorear su funcionamiento para detectar y atender anomalías y disfunciones lo antes posible
2. Decidir no utilizar el sistema de IA o ignorar, anular o revertir la salida del sistema de IA
3. Garantizar que el usuario/a no tome ninguna medida o decisión sobre el sistema, a menos que haya sido verificada y confirmada por al menos dos personas
4. Intervenir en el funcionamiento del sistema de IA

7) Precisión, robustez y ciberseguridad

Sistemas diseñados y desarrollados de manera de alcanzar un nivel adecuado de precisión, robustez y ciberseguridad, a lo largo del ciclo de vida

Sistemas de alto riesgo resistentes a errores, fallas o incoherencias

Medidas de mitigación para aquellos sistemas que continúen aprendiendo luego de ser comercializados para abordar resultados sesgados

Obligaciones de los proveedores/as de sistemas de IA de alto riesgo

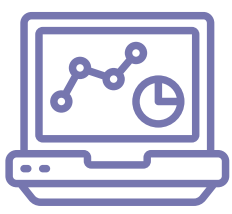
Garantizar que se cumplan los requisitos de los sistemas de IA de alto riesgo y tomar las acciones correctivas necesarias cuando estos requisitos no se cumplan

Elaborar documentación técnica del sistema, mantener los registros generados automáticamente por los sistemas de IA de alto riesgo y cumplir con las obligaciones de registro

Garantizar el procedimiento de evaluación del sistema de IA de alto riesgo, de manera previa a su comercialización o puesta en servicio

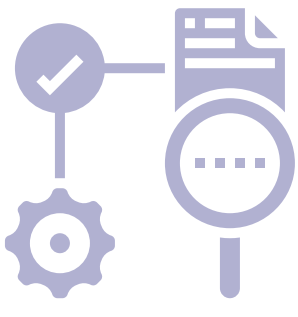
Deber de información y cooperación con las autoridades competentes. Deben informar y notificar a las autoridades y/u organismos correspondientes las medidas correctoras adoptadas y la aparición de riesgos en los sistemas de IA que puedan ocasionar daños para la salud o seguridad o para la protección de los derechos fundamentales de las personas

Establecer un sistema de gestión de calidad que garantice el cumplimiento del Reglamento (procedimientos de evaluación, técnicas, diseño, control, gestión de datos, verificación antes, durante y después del desarrollo del sistema de IA de alto riesgo)



Demostrar, ante el pedido de una autoridad competente, que el sistema cumple con los requisitos

Mantener a disposición de las autoridades competentes durante 10 años la documentación técnica; la documentación relativa al sistema de gestión de calidad, a los cambios aprobados por los organismos notificados; las decisiones y otros documentos emitidos por los organismos notificados y la declaración de conformidad a la UE



Establecer y documentar un sistema de seguimiento posterior a la comercialización del sistema de inteligencia artificial de alto riesgo

Obligaciones de los/as fabricantes de productos

El/la fabricante del producto es responsable de la conformidad del sistema de IA con el Reglamento y, en lo que respecta al sistema de IA, tiene las mismas obligaciones que los/as proveedores/as

Obligaciones de distribuidores/as, importadores/as, usuario/as o cualquier otro/a tercero/a

Están sujetos a las mismas obligaciones que los/as proveedores/as siempre que:

1. Comercialicen o pongan en servicio un sistema de IA de alto riesgo bajo su nombre o marca comercial
2. Modifiquen la finalidad prevista de un sistema IA de alto riesgo ya comercializado o puesto en servicio
3. Realicen una una modificación sustancial al sistema de IA de alto riesgo

Obligaciones de los usuarios/as

Usar y monitorear el sistema de conformidad a las instrucciones de uso

Informar al proveedor/a o distribuidor/a y suspender el uso del sistema cuando consideren que puede dar lugar a un riesgo o cuando presente un incidente grave o mal funcionamiento

Mantener los registros generados automáticamente por ese sistema de IA de alto riesgo que estén bajo su control

Autoridades de notificación

Cada Estado miembro establecerá una autoridad notificante responsable de establecer y llevar a cabo los procedimientos para la evaluación, designación y notificación de los organismos de evaluación, de conformidad y seguimiento

Excepción a la evaluación de conformidad

La autoridad podrá autorizar (por tiempo limitado) la comercialización o la puesta en servicio de sistemas de IA de alto riesgo que no cuenten con la evaluación de conformidad por razones excepcionales de seguridad pública o protección de la vida y salud de las personas, protección del medio ambiente y protección de activos industriales y de infraestructura clave

Registro del sistema de IA de alto riesgo

Antes de comercializar o poner en servicio un sistema de IA de alto riesgo, el/la proveedor/a o el/la representante autorizado/a deben registrar el sistema en la base de datos de la UE

Obligaciones de transparencia para ciertos sistemas de IA

Sistemas de IA destinados a interactuar con personas humanas: asegurar que sean diseñados y desarrollados de manera que las personas sepan de que están interactuando con un sistema de IA, a menos que sea obvio por las circunstancias y el contexto de uso

Excepción: sistemas de IA para detectar, prevenir, investigar y perseguir delitos, a menos que estén disponibles para que el público pueda denunciar un delito

Sistemas de IA de reconocimiento de emociones o de categorización biométrica: los/as usuarios/as deben informar del funcionamiento del sistema a las personas expuestas al mismo

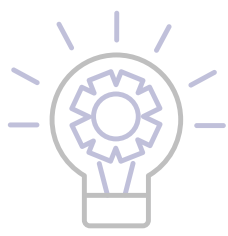
Excepción: sistemas de IA usados para la categorización biométrica que están permitidos por ley para detectar, prevenir e investigar delitos

Usuarios/as de un sistema de IA que genere o manipule contenido de imagen, audio o video que se parezca a personas, objetos, lugares, que parezca auténtico o veraz a una persona, deberán informar que ha sido generado artificialmente

Excepción: uso autorizado por ley para detectar, prevenir, investigar y perseguir delitos o su uso sea necesario para el ejercicio del derecho a la libertad de expresión y a la libertad de las artes y las ciencias garantizados en la Carta de derechos de la UE

Sandboxes regulatorios de IA

Los sandboxes no afectarán las facultades de supervisión y corrección de las autoridades competentes



Cualquier riesgo significativo para la salud, seguridad y derechos fundamentales identificado durante el desarrollo y prueba dará lugar a una mitigación inmediata

Los participantes del sandbox son responsables por cualquier daño infligido a terceros como resultado de la experimentación; coordinarán sus actividades con la Junta Europea de IA y presentarán informes anuales a la Junta y a la Comisión sobre los resultados, buenas prácticas, experiencia adquirida y recomendaciones

Procesamiento adicional de datos personales para el desarrollo de sistemas de IA para la prevención, investigación, o detección de infracciones penales o ejecución de sanciones penales; para la seguridad pública y salud pública; para brindar un un alto nivel de protección y mejora de la calidad del medio ambiente

Todos los datos personales procesados en este contexto estarán en un entorno funcionalmente separado, aislado y protegido y se eliminarán una vez que finalice el sandbox o cuando haya llegado al final de su período de retención

Creación de la Junta Europea de IA

Brinda asesoramiento y asistencia con el fin de:

- contribuir a la cooperación eficaz entre las autoridades nacionales de supervisión y la Comisión
- coordinar y contribuir a la orientación, análisis y supervisión del Reglamento
- ayudar a garantizar el cumplimiento del Reglamento

Tareas

1. Recopilar y compartir conocimientos y mejores prácticas

2. Coordinar y contribuir a la orientación, análisis y supervisión del Reglamento

3. Emitir dictámenes o recomendaciones sobre asuntos relacionados a la aplicación del Reglamento

Autoridades nacionales competentes

Cada Estado miembro establecerá autoridades competentes que garanticen la aplicación y ejecución del Reglamento, quienes deberán salvaguardar la objetividad e imparcialidad de sus actividades y garantizar la confidencialidad de la información y datos obtenidos, modo que se protejan:

-derechos de propiedad intelectual e información confidencial o comercial
-intereses públicos o de seguridad pública
-la aplicación efectiva del Reglamento
-integridad de los procedimientos penales o administrativos

Códigos de conducta

Se fomentará y facilitará la elaboración de códigos de conducta para fomentar la aplicación voluntaria de sistemas de IA distintos de los sistemas de alto riesgo (sistemas relacionados con sostenibilidad medioambiental, la accesibilidad de las personas con discapacidad). Pueden ser creados por proveedores/as, incluso con la participación de usuarios/as y partes interesadas

Infografía del Plan de IA

Informe completo