Parlamento Europeo
2019-2024

TEXTOS ADOPTADOS

P9_TA(2024)0138

Ley de Inteligencia Artificial

Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la inteligencia artificial (Ley sobre la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))

(Procedimiento legislativo ordinario: primera lectura)

El Parlamento Europeo,

– Vista la propuesta de la Comisión al Parlamento y al Consejo (COM(2021)0206),

– Vistos el apartado 2 del artículo 294 y los artículos 16 y 114 del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C9-0146/2021),

– Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,

– Visto el dictamen del Banco Central Europeo de 29 de diciembre de [1],

– Visto el dictamen del Comité Económico y Social Europeo de 22 de septiembre de [2],

– Visto el acuerdo provisional aprobado por las comisiones competentes, de conformidad con el apartado 4 del artículo 74 de su Reglamento, y el compromiso asumido por el representante del Consejo, mediante carta de 2 de febrero de 2024, de aprobar la posición del Parlamento, de conformidad con el apartado 4 del artículo 294 del Tratado de Funcionamiento de la Unión Europea,

– Visto el artículo 59 de su Reglamento,

– Vistas las deliberaciones conjuntas de la Comisión de Mercado Interior y Protección del Consumidor y de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de conformidad con el artículo 58 del Reglamento,

– Vista la opinión de la Comisión de Industria, Investigación y Energía, de la Comisión de Cultura y Educación, de la Comisión de Asuntos Jurídicos, de la Comisión

---

1 DO C 115 de 11.3.2022, p. 5.
2 DO C 517 de 22.12.2021, p. 56.

de Medio Ambiente, Salud Pública y Seguridad Alimentaria y la Comisión de Transportes y Turismo,

– Visto el informe de la Comisión de Mercado Interior y Protección del Consumidor y de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A9- 0188/2023),

1. Adopta su posición en primera lectura que figura a continuación[3];

2. 4. Pide a la Comisión que le consulte de nuevo, si sustituye, modifica sustancialmente o se propone modificar sustancialmente su propuesta;

3. Encarga a su Presidente que transmita la posición del Parlamento al Consejo, a la Comisión y a los Parlamentos nacionales.

[3] Esta posición sustituye a las enmiendas aprobadas el 14 de junio de 2023 (Textos Aprobados, P9_TA(2023)0236.

P9_TC1-COD(2021)0106

Posición del Parlamento Europeo adoptada en primera lectura el 13 de marzo de 2024 con vistas a la adopción del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial y se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE)
2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial)*.

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[1], ***Visto el dictamen del Banco Central Europeo[2],***

Visto el dictamen del Comité de las Regiones[3], De conformidad con el procedimiento legislativo ordinario[4],

---

* EL TEXTO AÚN NO HA SIDO OBJETO DE UNA FORMALIZACIÓN JURÍDICO-LINGÜÍSTICA.

1 DO C 517 de 22.12.2021, p. 56.

2 DO C 115 de 11.3.2022, p. 5.

3 DO C 97 de 28.2.2022, p. 60.

4 Posición del Parlamento Europeo de 13 de marzo de 2024.

Considerando que:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior estableciendo un marco jurídico uniforme, en particular para el desarrollo, la ***comercialización, la puesta en servicio y la*** utilización de ***sistemas de inteligencia artificial (***sistemas de IA***) en la Unión,*** de conformidad con los valores de la Unión***, promover la adopción de la inteligencia artificial (IA) centrada en el ser humano y digna de confianza, garantizando al mismo tiempo*** un alto nivel de protección de la salud, la seguridad***,*** los derechos fundamentales ***consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (la "Carta")***, ***incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, contra los efectos nocivos de los sistemas de IA en la Unión, y apoyar la innovación. El presente Reglamento*** garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA, impidiendo así que los Estados miembros impongan restricciones al desarrollo, la comercialización y el uso de sistemas de ***IA***, a menos que el presente Reglamento lo autorice explícitamente.

(2) El presente Reglamento debe aplicarse de conformidad con los valores de la Unión consagrados como en la Carta, facilitando la protección de las personas físicas, las empresas, la democracia, el Estado de Derecho y la protección del medio ambiente, impulsando al mismo tiempo la innovación y el empleo y haciendo de la Unión un líder en la adopción de la IA fiable.

(3) ▌ Los sistemas de IA ▌ pueden desplegarse fácilmente en una gran variedad de sectores de la economía y en muchas partes de la sociedad, incluso a través de las fronteras, y pueden circular fácilmente por toda la Unión. Algunos Estados miembros ya han estudiado la adopción de normas nacionales para garantizar que la IA sea ***digna de confianza y*** segura y se desarrolle y utilice de conformidad con las obligaciones en materia de derechos fundamentales. La existencia de normas nacionales divergentes puede conducir a la fragmentación del mercado interior y disminuir la seguridad jurídica de los operadores que desarrollan***, importan*** o utilizan sistemas de IA. Por consiguiente, debe garantizarse un nivel de protección coherente y elevado en toda la Unión para ***lograr una IA digna de confianza, al*** tiempo que deben evitarse las divergencias que obstaculizan la libre circulación***, la innovación, el despliegue y la adopción de sistemas de*** IA y productos y servicios relacionados dentro del mercado interior, estableciendo obligaciones uniformes para los operadores y garantizando la protección uniforme de las razones imperiosas de interés público y de los derechos de las personas en todo el mercado interior sobre la base del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). En la medida en que el presente Reglamento contiene normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales relativos a las restricciones de la utilización de sistemas de IA para la identificación biométrica a distancia a efectos de la aplicación ***de la ley, de la utilización de sistemas de IA para la evaluación del riesgo de las personas físicas a efectos de la aplicación de la ley y de la utilización de sistemas de IA de categorización biométrica*** a efectos de la aplicación de la ley, procede basar el presente Reglamento, en lo que respecta a dichas normas específicas, en el artículo 16 del TFUE. A la luz de esas normas específicas y del recurso al artículo 16 del TFUE, procede consultar al Consejo Europeo de Protección de Datos.

(4) La IA es una familia de tecnologías en rápida evolución que ***contribuye*** a una amplia gama de beneficios económicos***, medioambientales*** y sociales en todo el espectro de industrias y actividades sociales. Al mejorar la predicción, optimizar las operaciones y la asignación de recursos, y personalizar las soluciones digitales disponibles para particulares y organizaciones, el uso de la IA puede proporcionar ventajas competitivas clave a las empresas y apoyar resultados social y ambientalmente beneficiosos, por ejemplo en la asistencia sanitaria, la agricultura, la ***seguridad alimentaria, la*** educación y la formación, los ***medios de comunicación, los deportes, la cultura, la*** gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia energética y de los recursos, la ***vigilancia del medio ambiente, la conservación y restauración de la biodiversidad y los ecosistemas*** y la mitigación del cambio climático y la adaptación al mismo***.***

(5) Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación específica***, uso y nivel de desarrollo tecnológico***, la IA puede generar riesgos y causar daños a los intereses públicos y a los derechos fundamentales protegidos por el Derecho de la Unión. Estos daños pueden ser materiales o inmateriales***, incluidos los daños físicos, psicológicos, sociales o económicos***.

(6) ***Dado el gran impacto que la IA puede tener en la sociedad y la necesidad de generar confianza, es vital que la IA y su marco regulador se desarrollen de acuerdo con los valores de la Unión consagrados en el artículo 2 del Tratado de la Unión Europea (TUE), los derechos y libertades fundamentales consagrados en los Tratados y, de conformidad con el artículo 6 del TUE, la Carta. Como requisito previo, la IA debe ser una tecnología centrada en el ser humano. Debe servir como herramienta para las personas, con el objetivo último de aumentar el bienestar humano.***

(7) ***Para garantizar un nivel coherente y elevado de protección de los intereses públicos en materia de salud, seguridad y derechos fundamentales, deben establecerse normas comunes para los sistemas de IA de alto riesgo. Dichas normas deben ser coherentes con la Carta, no discriminatorias y acordes con los compromisos comerciales internacionales de la Unión. También deberían tener en cuenta la Declaración Europea sobre Derechos y Principios Digitales para la Década Digital y las directrices éticas para una IA digna de confianza del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (AI HLEG).***

(8) Por consiguiente, es necesario un marco jurídico de la Unión que establezca normas armonizadas en materia de IA para fomentar el desarrollo, la utilización y la adopción de la IA en el mercado interior que, al mismo tiempo, responda a un elevado nivel de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, ***incluidos la democracia, el Estado de Derecho y la protección del medio ambiente***, tal como se reconocen y protegen en el Derecho de la Unión. Para alcanzar ese objetivo, deben establecerse normas que regulen la comercialización***, la*** puesta en servicio ***y la utilización*** de determinados sistemas de IA, garantizando así el buen funcionamiento del mercado interior y permitiendo que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios. ***Esas normas deben ser claras y sólidas en la protección de los derechos fundamentales, apoyar las nuevas soluciones innovadoras, permitir un ecosistema europeo de agentes públicos y privados que creen sistemas de IA en consonancia con los valores de la Unión y liberar el potencial de la transformación digital en todas las regiones de la Unión.*** Al establecer esas normas, ***así como medidas de apoyo a la innovación con especial atención a las pequeñas y medianas empresas (PYME), incluidas las empresas emergentes***, el presente Reglamento apoya el objetivo de ***promover el enfoque europeo de la IA centrado en el ser humano y de*** ser un líder mundial en el desarrollo de una IA segura, fiable y ética ▌, tal como declaró el **Consejo** Europeo5, y garantiza la protección de los principios éticos, tal como solicitó específicamente ***el*** Parlamento **Europeo6**.

---

5 Consejo Europeo, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) - Conclusiones, EUCO 13/20, 2020, p. 6.

6 Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012(INL).

(9) Deben establecerse normas armonizadas aplicables a la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA de alto riesgo de conformidad con el Reglamento (CE) nº 765/2008 del Parlamento Europeo y del **Consejo7** , la Decisión nº 768/2008/CE del Parlamento Europeo y del **Consejo8** y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del **Consejo9** ("nuevo marco legislativo"). ***Las normas armonizadas establecidas en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con el nuevo marco legislativo, deben entenderse sin perjuicio de la legislación vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo y protección de los trabajadores, y seguridad de los productos, de la que el presente Reglamento es complementario.***

---

7 Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93 (DO L 218 de 13.8.2008,
p. 30).

8 Decisión nº 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

9 Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre vigilancia del mercado y conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 (Texto pertinente a efectos del EEE) (DO L 169 de 25.6.2019, p. 1-44).

En consecuencia, todos los derechos y vías de recurso previstos por el Derecho de la Unión para los consumidores y otras personas sobre las que los sistemas de IA puedan tener un impacto negativo, incluido lo relativo a la indemnización por posibles daños y perjuicios de conformidad con la Directiva 85/374/CEE del Consejo10 , no se verán afectados y serán plenamente aplicables. Además, en el contexto del empleo y la protección de los trabajadores, el presente Reglamento no debe afectar, por tanto, al Derecho de la Unión en materia de política social ni al Derecho laboral nacional, de conformidad con el Derecho de la Unión, relativo al empleo y las condiciones de trabajo, incluidas la salud y la seguridad en el trabajo y la relación entre empresarios y trabajadores. El presente Reglamento tampoco debe afectar al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluido el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas específicos de relaciones laborales de los Estados miembros, así como el derecho a negociar, celebrar y aplicar convenios colectivos o a emprender acciones colectivas de conformidad con el Derecho nacional.

10 Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (DO

L 210 de 7.8.1985, p. 29).

El presente Reglamento no debe afectar a las disposiciones destinadas a mejorar las condiciones laborales en el trabajo de plataforma establecidas en la Directiva (UE) 2024/... del Parlamento Europeo y del Consejo11+. Además, el presente Reglamento tiene por objeto reforzar la eficacia de los derechos y recursos existentes mediante el establecimiento de requisitos y obligaciones específicos, en particular en materia de transparencia, documentación técnica y registro de los sistemas de IA. Además, las obligaciones impuestas a los distintos operadores que intervienen en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio de la legislación nacional, de conformidad con el Derecho de la Unión, que tenga por efecto limitar el uso de determinados sistemas de IA cuando dicha legislación quede fuera del ámbito de aplicación del presente Reglamento o persiga otros objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Por ejemplo, el Derecho laboral nacional y el Derecho relativo a la protección de los menores, es decir, de las personas menores de 18 años, teniendo en cuenta la Observación general n.º 25 (2021) de las Naciones Unidas sobre los derechos del niño en relación con el entorno digital, en la medida en que no sean específicos de los sistemas de IA y persigan otros objetivos legítimos de interés público, no deben verse afectados por el presente Reglamento.

---

11 Directiva (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., relativa a la mejora de las condiciones de trabajo sobre plataformas (DO L, ..., ELI: ...).

\+ DO: por favor, inserte en el texto el número de la Directiva en PE XX/YY (2021/0414(COD)) y complete la nota a pie de página correspondiente.

(10) El derecho fundamental a la protección de los datos personales está salvaguardado, en particular, por los Reglamentos (UE) 2016/679[12] y (UE) 2018/1725[13] del Parlamento Europeo y del Consejo y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[14]. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo[15] protege además la vida privada y la confidencialidad de las comunicaciones, incluso mediante el establecimiento de condiciones para el almacenamiento de datos personales y no personales en equipos terminales y el acceso a los mismos. Estos actos jurídicos de la Unión sientan las bases para un tratamiento de datos sostenible y responsable, incluso cuando los conjuntos de datos incluyen una combinación de datos personales y no personales. El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de control independientes competentes para supervisar el cumplimiento de dichos instrumentos.

---

12 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

13 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

14 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de estos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

15 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

Tampoco afecta a las obligaciones de los proveedores e implantadores de sistemas de IA en su papel de responsables o encargados del tratamiento derivadas del Derecho de la Unión o nacional en materia de protección de datos personales en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales. También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les otorga dicho Derecho de la Unión, incluidos los derechos relacionados únicamente con la toma de decisiones individuales automatizadas, incluida la elaboración de perfiles. Las normas armonizadas para la comercialización, la puesta en servicio y el uso de los sistemas de IA establecidos en virtud del presente Reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos de los interesados y otras vías de recurso garantizadas por el Derecho de la Unión en materia de protección de datos personales y de otros derechos fundamentales.

(11) El presente Reglamento debe entenderse sin perjuicio de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en la Directiva 2000/31/CE del Parlamento Europeo y del *Consejo16*.

16 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior ("Directiva

sobre el comercio electrónico") (DO L 178 de 17.7.2000, p. 1).

(12) La noción de ***"***sistema de IA" ***en el presente Reglamento*** debe definirse claramente ***y debe ajustarse estrechamente a la labor de las organizaciones internacionales que trabajan en el ámbito de la IA*** para garantizar la seguridad jurídica, ***facilitar la convergencia internacional y una amplia aceptación,*** proporcionando al mismo tiempo la flexibilidad necesaria para adaptarse a ***la rápida*** evolución tecnológica ***en este ámbito. Además,*** debe basarse en las características clave de los sistemas de IA ***que los distinguen de los sistemas de software tradicionales más sencillos o de los enfoques de programación y no debe abarcar los sistemas que se basan en las reglas definidas únicamente por personas físicas para ejecutar operaciones automáticamente. Una característica clave de los sistemas de IA es su capacidad de inferencia. Esta capacidad de inferencia se refiere al proceso de obtención de*** resultados***,*** como ***predicciones, contenidos***, recomendaciones o decisiones***,*** que ***pueden*** influir en ***entornos físicos y virtuales, y a una capacidad de los sistemas de IA para derivar modelos o algoritmos a partir de entradas o datos. Las técnicas que permiten inferir al construir un sistema de IA incluyen enfoques de aprendizaje automático que aprenden a partir de los datos cómo alcanzar determinados objetivos, y enfoques basados en la lógica y el conocimiento que infieren a partir del conocimiento codificado o la representación simbólica de la tarea a resolver. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos y permite el aprendizaje, el razonamiento o la modelización. El término "basado en máquinas" se refiere al hecho de que los sistemas de IA funcionan en máquinas.***

La referencia a objetivos explícitos o implícitos subraya que los sistemas de IA pueden funcionar con arreglo a objetivos explícitos definidos o a objetivos implícitos. Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico***. A efectos del presente Reglamento,*** debe entenderse ***que los entornos son los contextos en los que operan los sistemas de IA, mientras que los resultados generados por el sistema de IA reflejan diferentes funciones realizadas por los sistemas de IA e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que tienen cierto grado de independencia de las acciones de la intervención humana y de capacidades para funcionar sin intervención humana. La capacidad de adaptación que puede mostrar un sistema de IA tras su despliegue se refiere a las capacidades de autoaprendizaje, que permiten al sistema cambiar mientras se utiliza. Los sistemas de IA pueden utilizarse de forma autónoma o como componente de un producto, independientemente de que el sistema esté integrado físicamente en el producto (integrado) o sirva a la funcionalidad del producto sin estar integrado en él (no integrado)***.

(13) El concepto de "responsable del despliegue" mencionado en el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida una autoridad pública, agencia u otro organismo, que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas de quien lo despliega.

(14) El concepto de ***"datos biométricos"*** utilizado en el presente Reglamento ▌ debe interpretarse a la ***luz*** del concepto de datos biométricos definido en el artículo 4, punto 14, del Reglamento (UE) 2016/679, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 y en el artículo 3, punto 13, de la Directiva (UE) 2016/680***. Los datos biométricos pueden permitir la autenticación, identificación o categorización de personas físicas y el reconocimiento de emociones de personas físicas.***

(15) La noción de "identificación biométrica" a que se refiere el presente Reglamento debe definirse como el reconocimiento automatizado de rasgos humanos físicos, fisiológicos y de comportamiento, como el rostro, el movimiento de los ojos, la forma del cuerpo, la voz, la prosodia, la marcha, la postura, la frecuencia cardíaca, la presión arterial, el olor, las características de las pulsaciones de teclas, con el fin de establecer la identidad de una persona comparando los datos biométricos de dicha persona con los datos biométricos almacenados de personas físicas en una base de datos de referencia, independientemente de que la persona física haya dado o no su consentimiento. Esto excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física específica es la persona que dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso de seguridad a locales.

(16) ***La noción de "categorización biométrica" a que se refiere el presente Reglamento debe definirse como la asignación de personas físicas a categorías específicas sobre la base de sus datos biométricos. Dichas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos de comportamiento o de personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política. Esto no incluye los sistemas de categorización biométrica que son una característica puramente auxiliar intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede, por razones técnicas objetivas, utilizarse sin el servicio principal y la integración de esa característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. Por ejemplo, los filtros que categorizan los rasgos faciales o corporales utilizados en los mercados en línea podrían constituir una característica accesoria de este tipo, ya que sólo pueden utilizarse en relación con el servicio principal, que consiste en vender un producto permitiendo al consumidor previsualizar la visualización del producto en sí mismo y ayudándole a tomar una decisión de compra. Los filtros utilizados en los servicios de redes sociales en línea que categorizan los rasgos faciales o corporales para permitir a los usuarios añadir o modificar imágenes o vídeos también podrían considerarse características accesorias, ya que dichos filtros no pueden utilizarse sin el servicio principal de los servicios de redes sociales, que consiste en compartir contenidos en línea.***

(17) La noción de ***"***sistema de identificación biométrica a distancia" a que se refiere el presente Reglamento debe definirse funcionalmente como un sistema de IA destinado a la identificación de personas físicas sin su participación ***activa, normalmente a*** distancia***,*** mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia, ***con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos utilizados. Estos sistemas de identificación biométrica a distancia se utilizan normalmente para percibir simultáneamente a varias personas o su comportamiento con el fin de facilitar de forma significativa la identificación de personas físicas*** sin ***su participación activa. Esto excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física específica es la persona que dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso de seguridad a locales. Esta exclusión se justifica por el hecho de que es probable que tales sistemas tengan un impacto menor en los derechos fundamentales de las personas físicas en comparación con los sistemas de identificación biométrica a distancia, que pueden utilizarse para el tratamiento de los datos*** biométricos ***de un gran número de personas sin su participación activa***. En el caso de los sistemas "en tiempo real", la captura de los datos biométricos, la comparación y la identificación se producen de forma instantánea, casi instantánea o, en cualquier caso, sin un retraso significativo. A este respecto, no debe haber margen para eludir las normas del presente Reglamento sobre el uso "en tiempo real" de los sistemas de IA en cuestión previendo retrasos menores. Los sistemas "en tiempo real" implican el uso de material "en directo" o "casi en directo", como imágenes de vídeo, generadas por una cámara u otro dispositivo con una funcionalidad similar. En cambio, en los sistemas "a posteriori", los datos biométricos ya se han capturado y la comparación y la identificación sólo se producen tras un retraso significativo. Se trata de material, como imágenes o secuencias de vídeo generadas por cámaras de circuito cerrado de televisión o dispositivos privados, que se ha generado antes de la utilización del sistema con respecto a las personas físicas en cuestión.

(18) ***La noción de "sistema de reconocimiento de emociones" a que se refiere el presente Reglamento debe definirse como un sistema de IA destinado a identificar o deducir emociones o intenciones de personas físicas a partir de sus datos biométricos. El concepto se refiere a emociones o intenciones como la felicidad, la tristeza, la ira, la sorpresa, el asco, la vergüenza, la excitación, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye estados físicos, como el dolor o la fatiga; se refiere, por ejemplo, a los sistemas utilizados para detectar el estado de fatiga de pilotos o conductores profesionales con el fin de prevenir accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos fácilmente aparentes, a menos que se utilicen para identificar o deducir emociones. Esas expresiones pueden ser gestos faciales básicos, como fruncir el ceño o sonreír, o gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como levantar la voz o susurrar.***

(19) A efectos del presente Reglamento, debe entenderse que la noción de "espacio de acceso público" se refiere a cualquier lugar físico que sea accesible a ***un número indeterminado de personas físicas, e independientemente de*** si el lugar en cuestión es de propiedad privada o pública, con ***independencia de la actividad para la que pueda utilizarse el lugar, como el comercio (por ejemplo, tiendas, restaurantes, cafés), servicios (por ejemplo, bancos, actividades profesionales, hostelería), deporte (por ejemplo, piscinas, gimnasios, estadios), transporte (por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte), ocio (por ejemplo, cines, teatros, museos, salas de conciertos y conferencias), u otras actividades (por ejemplo, vías y plazas públicas, parques, bosques, zonas de juegos)***. ***Un lugar debe clasificarse como de acceso público también si, independientemente de las posibles restricciones de capacidad o seguridad, el acceso está sujeto a*** ciertas condiciones ***predeterminadas, que pueden cumplir un número indeterminado de personas***, como la ***compra de un billete o título de transporte, el registro previo o tener una determinada edad. Por el contrario, un lugar no debe considerarse de acceso público si el acceso está limitado a personas físicas concretas y definidas, ya sea mediante legislación de la Unión o nacional directamente relacionada con la seguridad pública o mediante la manifestación clara de voluntad de la persona que tiene la autoridad pertinente sobre el lugar. La posibilidad fáctica de acceso por sí sola (como una puerta sin cerrar o una puerta abierta en una valla)*** no ***implica*** que el ***lugar sea*** accesible al público ***en presencia de indicios o circunstancias que sugieran lo contrario (como. señales que prohíban o restrinjan el acceso). Los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que sólo pueden acceder los empleados y proveedores de servicios*** pertinentes***, son lugares que no son accesibles al público. Los espacios de acceso público no deben incluir prisiones ni controles fronterizos. Algunos otros espacios pueden estar compuestos tanto de espacios no accesibles al público como de espacios accesibles al público,*** como ***el pasillo de un edificio residencial privado necesario para acceder a la consulta de un médico o a un aeropuerto. Los espacios en línea tampoco están cubiertos, ya que no son espacios físicos***. No obstante, la cuestión de si un espacio determinado es accesible al público debe determinarse caso por caso, teniendo en cuenta las especificidades de la situación concreta de que se trate.

(20) ***Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y para permitir el control democrático, la alfabetización en materia de IA debe dotar a los proveedores, implantadores y personas afectadas de las nociones necesarias para tomar decisiones con conocimiento de causa en relación con los sistemas de IA. Estas nociones pueden variar en función del contexto pertinente y pueden incluir la comprensión de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados del sistema de IA y, en el caso de las personas afectadas, los conocimientos necesarios para comprender cómo les afectarán las decisiones adoptadas con ayuda de la IA. En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el adecuado cumplimiento y su correcta aplicación. Además, la aplicación generalizada de las medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, a sostener la consolidación y la senda de innovación de una IA fiable en la Unión. La Junta Europea de Inteligencia Artificial (la "Junta") debe apoyar a la Comisión en la promoción de herramientas de alfabetización en IA, la concienciación pública y la comprensión de los beneficios, riesgos, salvaguardias, derechos y obligaciones en relación con el uso de sistemas de IA. En cooperación con las partes interesadas pertinentes, la Comisión y los Estados miembros deben facilitar la elaboración de códigos de conducta voluntarios para fomentar la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el funcionamiento y el uso de la IA.***

(21) Para garantizar la igualdad de condiciones y una protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas por el presente Reglamento deben aplicarse a los proveedores de sistemas de IA de forma no discriminatoria, con independencia de que estén establecidos en la Unión o en un tercer país, y a los ***implantadores*** de sistemas de IA establecidos en la Unión.

(22) Habida cuenta de su naturaleza digital, determinados sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento incluso cuando no se comercialicen, pongan en servicio o utilicen en la Unión. Este es el caso, por ejemplo, cuando un operador establecido en la Unión contrata determinados servicios a un operador establecido en un tercer país en relación con una actividad que debe realizar un sistema de IA que se calificaría de alto riesgo ▌. En tales circunstancias, el sistema de IA utilizado en un tercer país por el operador podría tratar datos recogidos legalmente en la Unión y transferidos desde esta, y proporcionar al operador contratante en la Unión el producto de dicho sistema de IA resultante de ese tratamiento, sin que dicho sistema de IA se comercialice, se ponga en servicio o se utilice en la Unión. Para evitar que se eluda el presente Reglamento y garantizar una protección efectiva de las personas físicas situadas en la Unión, el presente Reglamento debe aplicarse también a los proveedores e ***implantadores*** de sistemas de IA que estén establecidos en un tercer país, en la medida en que el resultado producido por dichos sistemas esté ***destinado a ser*** utilizado en la Unión.

No obstante, para tener en cuenta los acuerdos existentes y las necesidades especiales de la ***futura*** cooperación con socios extranjeros con los que se intercambien información y pruebas, el presente Reglamento no debe aplicarse a las autoridades públicas de un tercer país y a las organizaciones internacionales cuando actúen en el marco de la ***cooperación o de*** acuerdos internacionales celebrados a escala de la Unión o nacional para la cooperación policial y judicial con la Unión o los Estados miembros***, siempre que el tercer país o las organizaciones internacionales de que se trate ofrezcan garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas. En su caso, esto puede abarcar las actividades de las entidades encargadas por los terceros países de llevar a cabo tareas específicas en apoyo de dicha cooperación policial y judicial. Tales marcos de cooperación o*** acuerdos se han ***establecido*** bilateralmente entre los Estados miembros y terceros países o entre la Unión Europea, Europol y otras agencias de la Unión y terceros países y organizaciones internacionales. ***Las autoridades competentes para la supervisión de las autoridades policiales y judiciales en virtud del presente Reglamento deben evaluar si dichos marcos de cooperación o acuerdos internacionales incluyen garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas.***

Las autoridades de los Estados miembros receptores y las instituciones, órganos y organismos de la Unión que utilicen dichos productos en la Unión son responsables de garantizar que su uso se ajuste al Derecho de la Unión. Cuando se revisen esos acuerdos internacionales o se celebren otros nuevos en el futuro, las partes contratantes deben hacer todo lo posible para adaptar dichos acuerdos a los requisitos del presente Reglamento.

(23) El presente Reglamento también debe aplicarse a las instituciones, órganos y organismos de la Unión cuando actúen como proveedores o ***implantadores*** de un sistema de IA. ▌

(24) En la medida en que los sistemas de IA se comercialicen, se pongan en servicio o se utilicen, con o sin modificación de dichos sistemas, con fines militares, de defensa o de seguridad nacional, deben quedar excluidos del ámbito de aplicación del presente Reglamento, con independencia del tipo de entidad que lleve a cabo dichas actividades, ya sea pública o privada. Por lo que se refiere a los fines militares y de defensa, dicha exclusión se justifica tanto por el artículo 4, apartado 2, del TUE como por las especificidades de la política de defensa de los Estados miembros y de la Unión común cubiertas por el capítulo 2 del título V del TUE que están sujetas al Derecho internacional público, que es, por tanto, el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de actividades militares y de defensa. Por lo que respecta a los fines de seguridad nacional, la exclusión se justifica tanto por el hecho de que la seguridad nacional sigue siendo responsabilidad exclusiva de los Estados miembros, de conformidad con el artículo 4, apartado 2, del TUE, como por la naturaleza específica y las necesidades operativas de las actividades de seguridad nacional y las normas nacionales específicas aplicables a dichas actividades. No obstante, si un sistema de IA desarrollado, comercializado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utiliza fuera de ellos, temporal o permanentemente, para otros fines, por ejemplo, civiles o humanitarios, policiales o de seguridad pública, dicho sistema entraría en el ámbito de aplicación del presente Reglamento.

En ese caso, la entidad que utilice el sistema para fines distintos de los militares, de defensa o de seguridad nacional deberá garantizar la conformidad del sistema con el presente Reglamento, a menos que el sistema ya sea conforme con el presente Reglamento. Los sistemas de IA comercializados o puestos en servicio para un fin excluido, a saber, militar, de defensa o de seguridad nacional, y uno o varios fines no excluidos, como fines civiles o policiales, entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento del presente Reglamento. En estos casos, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del presente Reglamento no debe afectar a la posibilidad de que las entidades que lleven a cabo actividades de seguridad nacional, defensa y militares, independientemente del tipo de entidad que lleve a cabo dichas actividades, utilicen sistemas de IA para fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento. Un sistema de IA comercializado con fines civiles o policiales que se utilice, con o sin modificaciones, con fines militares, de defensa o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo dichas actividades.

(25) ***El presente Reglamento debe apoyar la innovación, respetar la libertad de la ciencia y no menoscabar la actividad de investigación y desarrollo. Por consiguiente, es necesario excluir de su ámbito de aplicación los sistemas y modelos de IA desarrollados y puestos en servicio específicamente con el único fin de la investigación y el desarrollo científicos. Además, es necesario garantizar que el presente Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su comercialización o puesta en servicio. Por lo que respecta a la actividad de investigación, ensayo y desarrollo orientada al producto en relación con los sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que dichos sistemas y modelos se pongan en servicio o se comercialicen. Esta exclusión se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando un sistema de IA que entre en el ámbito de aplicación del mismo se comercialice o se ponga en servicio como resultado de dicha actividad de investigación y desarrollo y de la aplicación de las disposiciones sobre los entornos aislados reglamentarios y los ensayos en condiciones reales. Además, sin perjuicio de la exclusión relativa a los sistemas de IA específicamente desarrollados y puestos en servicio con el único fin de la investigación y el desarrollo científicos, cualquier otro sistema de IA que pueda utilizarse para la realización de cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier caso, cualquier actividad de investigación y desarrollo debe llevarse a cabo de conformidad con las normas éticas y profesionales reconocidas para la investigación científica y debe realizarse de conformidad con la legislación aplicable de la Unión.***

(26) Para introducir un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, debe seguirse un enfoque basado en el riesgo claramente definido. Ese enfoque debe adaptar el tipo y el contenido de tales normas a la intensidad y el alcance de los riesgos que pueden generar los sistemas de IA. Por lo tanto, es necesario prohibir determinadas prácticas de IA ***inaceptables***, establecer requisitos para los sistemas de IA de alto riesgo y obligaciones para los operadores correspondientes, y establecer obligaciones de transparencia para determinados sistemas de IA.

(27) Si bien el enfoque basado en el riesgo es la base de un conjunto proporcionado y eficaz de normas vinculantes, es importante recordar las directrices éticas de 2019 para una IA digna de confianza elaboradas por el HLEG independiente de IA nombrado por la Comisión. En esas directrices, el HLEG de IA desarrolló siete principios éticos no vinculantes para la IA que pretenden ayudar a garantizar que la IA sea digna de confianza y éticamente sólida. Los siete principios incluyen la agencia y la supervisión humanas; la solidez técnica y la seguridad; la privacidad y la gobernanza de los datos; la transparencia; la diversidad, la no discriminación y la equidad; el bienestar social y medioambiental y la responsabilidad. Sin perjuicio de los requisitos jurídicamente vinculantes del presente Reglamento y de cualquier otra legislación aplicable de la Unión, esas directrices contribuyen al diseño de una IA coherente, digna de confianza y centrada en el ser humano, en consonancia con la Carta y con los valores en los que se fundamenta la Unión. Según las directrices del HLEG sobre IA, la agencia y la supervisión humanas significan que los sistemas de IA se desarrollan y utilizan como una herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que puede ser controlada y supervisada adecuadamente por los seres humanos.

Solidez y seguridad técnicas significa que los sistemas de IA se desarrollan y utilizan de forma que sean sólidos en caso de problemas y resistentes frente a los intentos de alterar el uso o el rendimiento del sistema de IA para permitir un uso ilícito por parte de terceros, y minimizar los daños no intencionados. La gobernanza de la privacidad y los datos significa que los sistemas de IA se desarrollan y utilizan de acuerdo con las normas de privacidad y protección de datos, al tiempo que procesan datos que cumplen altos estándares en términos de calidad e integridad.

Transparencia significa que los sistemas de IA se desarrollan y utilizan de forma que permitan una trazabilidad y explicabilidad adecuadas, al tiempo que se informa a los seres humanos de que se comunican o interactúan con un sistema de IA, así como se informa debidamente a los usuarios de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas de sus derechos. Diversidad, no discriminación y equidad significa que los sistemas de IA se desarrollan y utilizan de forma que incluyan a diversos actores y promuevan la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los impactos discriminatorios y los sesgos injustos prohibidos por el Derecho de la Unión o nacional. Bienestar social y medioambiental significa que los sistemas de IA se desarrollan y utilizan de forma sostenible y respetuosa con el medio ambiente, así como de manera que beneficien a todos los seres humanos, al tiempo que se supervisan y evalúan los impactos a largo plazo sobre el individuo, la sociedad y la democracia. La aplicación de estos principios debe traducirse, cuando sea posible, en el diseño y uso de modelos de IA. En cualquier caso, deben servir de base para la elaboración de códigos de conducta en el marco del presente Reglamento. Se anima a todas las partes interesadas, incluidos la industria, el mundo académico, la sociedad civil y las organizaciones de normalización, a tener en cuenta, según proceda, los principios éticos para el desarrollo de mejores prácticas y normas voluntarias.

(28) Aparte de los muchos usos beneficiosos de la IA, esa tecnología también puede utilizarse indebidamente y proporcionar herramientas novedosas y poderosas para prácticas de manipulación, explotación y control social. Tales prácticas son especialmente dañinas y ***abusivas y*** deben prohibirse porque contradicen los valores de la Unión de respeto a la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y los derechos fundamentales consagrados en la Carta, incluido el derecho a la no discriminación, a la protección de datos y a la intimidad y los derechos del niño.

(29) ***Las técnicas de manipulación basadas en la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados, o para engañarlas induciéndolas a tomar decisiones que subviertan y menoscaben su autonomía, su capacidad de decisión y su libre elección.*** La comercialización, la puesta en servicio o el uso de determinados sistemas de IA ***con el objetivo o el efecto de distorsionar materialmente*** el comportamiento humano, mediante los cuales es probable que se produzcan ***daños significativos, en particular con repercusiones adversas suficientemente importantes en la salud*** física ***o psicológica o en los intereses financieros***, ***son especialmente peligrosos y, por lo tanto,*** deben prohibirse. Tales sistemas de IA utilizan componentes subliminales***, como estímulos de audio, imagen o vídeo que las personas*** no pueden percibir, ***ya que dichos estímulos están más allá de la percepción humana, u otras técnicas manipuladoras o engañosas que subvierten o menoscaban la autonomía, la toma de decisiones o la libre elección de las personas de forma que éstas no son conscientes o, cuando son conscientes, siguen siendo engañadas o no son capaces de controlar o resistir. Esto podría verse facilitado, por ejemplo, por las interfaces máquina-cerebro o la realidad virtual, ya que permiten un mayor grado de control de los estímulos que se presentan a las personas, en la medida en que pueden distorsionar materialmente su comportamiento de forma significativamente perjudicial. Además, los sistemas de IA también pueden*** explotar ***de otro modo*** las vulnerabilidades de ***una persona o un grupo específico de personas*** debido a su edad, ***discapacidad en el sentido de la Directiva (UE) 2019/882 del Parlamento Europeo y del*** *Consejo17*, ***o una situación social o económica específica que probablemente haga que esas personas sean más vulnerables a la explotación, como las personas que viven en condiciones de extrema pobreza o las minorías étnicas o religiosas.***

[17] Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativa a los requisitos de accesibilidad de productos y servicios (DO L 151 de 7.6.2019, p. 70).

Tales sistemas de IA pueden comercializarse, ponerse en servicio o utilizarse con el ***objetivo o el efecto de distorsionar*** materialmente el comportamiento de una persona y de una manera que cause o sea ***razonablemente*** probable que cause un daño significativo a esa u otra persona ***o grupos de personas, incluidos los daños que puedan acumularse a lo largo del tiempo y que, por lo tanto, deben prohibirse***. Puede que no sea posible suponer que existe la intención ***de distorsionar el comportamiento*** cuando la distorsión ▌ resulte de factores externos al sistema de IA que escapen al control del ***proveedor o del implantador, a saber, factores que pueden no ser razonablemente previsibles y, por tanto, no ser posibles de mitigar por el proveedor o el implantador del sistema de IA. En cualquier caso, no es necesario que el proveedor o el implantador tengan la intención de causar un daño significativo, siempre que dicho daño se derive de las prácticas manipuladoras o explotadoras basadas en la IA. Las prohibiciones de tales prácticas de IA son complementarias de las disposiciones contenidas en la Directiva 2005/29/CE del Parlamento Europeo y del*** *Consejo*[18]***, en particular las prácticas comerciales desleales que conducen a perjuicios económicos o financieros para los consumidores están prohibidas en todas las circunstancias, independientemente de si se ponen en práctica a través de sistemas de IA o de otro modo. Las prohibiciones de prácticas manipuladoras y explotadoras del presente Reglamento no deben afectar a las prácticas lícitas en el contexto del tratamiento médico, como el tratamiento psicológico de una enfermedad mental o la rehabilitación física, cuando dichas prácticas se lleven a cabo*** de conformidad con ***la legislación y las*** normas ***médicas aplicables, por ejemplo el consentimiento explícito de las personas o de sus representantes legales. Además, las prácticas comerciales comunes y legítimas, por ejemplo en el ámbito de la publicidad, que se ajusten a la legislación aplicable no deben considerarse, en sí mismas, constitutivas de prácticas manipuladoras nocivas de la IA***.

---

18 Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo ("Directiva sobre las prácticas comerciales desleales") (DO L 149 de 11.6.2005, p. 22).

(30) ***Deben prohibirse los sistemas de categorización biométrica que se basen en datos biométricos de personas físicas, como el rostro o las huellas dactilares de una persona, para deducir o inferir las opiniones políticas, la afiliación sindical, las creencias religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona. Dicha prohibición no debe abarcar el etiquetado, filtrado o categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho de la Unión o nacional en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o de los ojos, que puede utilizarse, por ejemplo, en el ámbito policial.***

(31) Los sistemas de IA que proporcionan una puntuación social de las personas físicas ▌ por parte de ***agentes*** públicos ***o privados*** pueden dar lugar a resultados discriminatorios y a la exclusión de determinados grupos. Pueden vulnerar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican a ***personas físicas o a grupos de ellas sobre la base*** de ***múltiples puntos de datos relacionados con*** su comportamiento social en múltiples contextos o características personales o de personalidad conocidas***, inferidas*** o predichas ***a lo largo de determinados periodos de tiempo***. La puntuación social obtenida de tales sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de personas físicas o grupos enteros de éstas en contextos sociales que no guardan relación con el contexto en el que se generaron o recopilaron originalmente los datos, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, deben prohibirse los ***sistemas de IA que conlleven tales prácticas de puntuación inaceptables y conduzcan a tales resultados perjudiciales o desfavorables***. ***Esta prohibición no debe afectar a las prácticas legales de evaluación de personas físicas que se lleven a cabo con un fin específico de conformidad con el Derecho de la Unión y nacional.***

(32) El uso de sistemas de IA para la identificación biométrica remota "en tiempo real" de personas físicas en espacios de acceso público con fines policiales es especialmente intrusivo ***para*** los derechos y libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de gran parte de la población, evocar una sensación de vigilancia constante y disuadir indirectamente del ejercicio de la libertad de reunión y otros derechos fundamentales. ***Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica a distancia de personas físicas pueden dar lugar a resultados sesgados y conllevar efectos discriminatorios. Estos posibles resultados sesgados y efectos discriminatorios son especialmente relevantes en relación con la edad, la etnia, la raza, el sexo o las discapacidades.*** Además, la inmediatez del impacto y las limitadas oportunidades de realizar comprobaciones o correcciones posteriores en relación con el uso de tales sistemas que operan en tiempo real conllevan mayores riesgos para los derechos y libertades de las personas que se ven afectadas por las actividades policiales.

(33) Por consiguiente, debe prohibirse el uso de dichos sistemas con fines policiales, salvo en situaciones enumeradas exhaustivamente y definidas con precisión, en las que el uso sea estrictamente necesario para lograr un interés público sustancial cuya importancia supere los riesgos. Dichas situaciones implican la búsqueda de ***determinadas*** víctimas de delitos ▌ incluidas ***las personas*** desaparecidas; determinadas amenazas para la vida o la seguridad física de personas físicas o de un atentado terrorista; y la localización ***o identificación*** de los autores o sospechosos de los delitos enumerados en un anexo del presente Reglamento***, cuando*** dichos delitos sean punibles con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos ***cuatro*** años en el Estado miembro de que se trate, de conformidad con la legislación de dicho Estado miembro. Dicho umbral para la pena privativa de libertad o la medida de seguridad privativa de libertad de conformidad con la legislación nacional contribuye a garantizar que el delito sea lo suficientemente grave como para justificar potencialmente el uso de sistemas de identificación biométrica a distancia "en tiempo real".

Además, ***estos delitos se basan en*** los 32 delitos enumerados en la Decisión marco 2002/584/JAI del ***Consejo19*** ***, teniendo en cuenta que***, en la práctica, es probable que algunos de estos delitos sean más pertinentes que otros, en el sentido de que el recurso a la identificación biométrica a distancia "en tiempo real" es, previsiblemente, necesario y proporcionado en grados muy diversos para la persecución práctica de la localización ***o identificación*** de un autor o sospechoso de los distintos delitos enumerados y teniendo en cuenta las diferencias probables en la gravedad, probabilidad y escala del daño o de las posibles consecuencias negativas. ***Una amenaza inminente para la vida o la seguridad física de las personas físicas también podría derivarse de una perturbación grave de infraestructuras críticas, tal como se definen en el artículo 2, punto (4) de la Directiva (UE) 2022/2557 del Parlamento Europeo y del*** *Consejo20* ***, cuando la perturbación o destrucción de dichas infraestructuras críticas diera lugar a una amenaza inminente para la vida o la seguridad física de una persona, incluso a través de un perjuicio grave para el abastecimiento básico de la población o para el ejercicio de la función esencial del Estado. Además, el presente Reglamento debe preservar la capacidad de las autoridades policiales, de control fronterizo, de inmigración o de asilo para llevar a cabo controles de identidad en presencia de la persona de que se trate, de conformidad con las condiciones establecidas en el Derecho de la Unión y nacional para dichos controles. En particular, las autoridades policiales, de control fronterizo, de inmigración o de asilo deben poder utilizar los sistemas de información, de conformidad con el Derecho de la Unión o nacional, para identificar a las personas que, durante un control de identidad, se nieguen a ser identificadas o no puedan declarar o probar su identidad, sin que el presente Reglamento les exija obtener una autorización previa. Puede tratarse, por ejemplo, de una persona implicada en un delito, que no quiera o no pueda, debido a un accidente o a un problema médico, revelar su identidad a las autoridades policiales.***

---

19 ***Decisión marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1).***

20 Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resistencia de las entidades críticas y por la que se deroga la Directiva

2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164).

(34) Para garantizar que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en cada una de esas situaciones enumeradas exhaustivamente y definidas de manera estricta, deben tenerse en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que da lugar a la solicitud y a las consecuencias de la utilización para los derechos y libertades de todas las personas afectadas, así como a las salvaguardias y condiciones previstas con la utilización. Además, el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales debe ***desplegarse únicamente para confirmar la identidad de la persona a la que se dirige específicamente y debe limitarse a lo estrictamente necesario en cuanto al período de tiempo y al ámbito geográfico y personal***, teniendo en cuenta en particular las pruebas o indicios relativos a las amenazas, las víctimas o el autor. La ***utilización del sistema de identificación biométrica a distancia en tiempo real en espacios de acceso público sólo debe autorizarse si la autoridad policial pertinente ha realizado una evaluación de impacto sobre los derechos fundamentales y, salvo disposición en contrario del presente Reglamento, ha registrado el sistema en la base de datos tal como se establece en el presente Reglamento. La base de datos*** de referencia de personas debe ser adecuada para cada caso de uso en cada una de las situaciones mencionadas anteriormente.

(35) Toda utilización de un sistema de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales debe estar sujeta a una autorización expresa y específica de una autoridad judicial o de una autoridad administrativa independiente ***cuya decisión sea vinculante*** para un Estado miembro. Dicha autorización debería obtenerse, en principio, antes de la ***utilización del sistema de IA con vistas a la identificación de una o varias personas. Deben permitirse excepciones a esta norma*** en situaciones debidamente justificadas por motivos de urgencia, es decir, en situaciones en las que la necesidad de utilizar los sistemas de que se trate sea tal que haga efectiva y objetivamente imposible obtener una autorización antes de comenzar a utilizar el sistema de IA. En tales situaciones de urgencia, el uso del sistema de IA debe limitarse al mínimo absolutamente necesario y debe estar sujeto a las salvaguardias y condiciones adecuadas, determinadas en la legislación nacional y especificadas en el contexto de cada caso individual de uso urgente por la propia autoridad policial. Además, en tales situaciones, las fuerzas y cuerpos de seguridad deben ***solicitar dicha*** autorización ▌ exponiendo los motivos por los que no han podido solicitarla antes***, sin demoras indebidas y, a más tardar, en un plazo de 24 horas. Si se deniega dicha autorización, debe cesar con efecto inmediato el uso de los sistemas de identificación biométrica en tiempo real vinculados a dicha autorización y deben descartarse y borrarse todos los datos relacionados con dicho uso. Dichos datos incluyen los datos de entrada adquiridos directamente por un sistema de IA en el curso de la utilización de dicho sistema, así como los resultados y productos de la utilización vinculada a dicha autorización. No deben incluirse los datos de entrada adquiridos legalmente de conformidad con otro Derecho de la Unión o nacional. En cualquier caso, no debe tomarse ninguna decisión que produzca un efecto jurídico adverso sobre una persona basándose únicamente en los resultados del sistema de identificación biométrica a distancia***.

(36) Con el fin de llevar a cabo sus tareas de conformidad con los requisitos establecidos en el presente Reglamento, así como en las normas nacionales, la autoridad de vigilancia del mercado pertinente y la autoridad nacional de protección de datos deben ser notificadas de cada uso del sistema de identificación biométrica en tiempo real. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos que hayan sido notificadas deben presentar a la Comisión un informe anual sobre el uso de los sistemas de identificación biométrica en tiempo real.

(37) Además, conviene prever, en el marco exhaustivo establecido por el presente Reglamento, que dicho uso en el territorio de un Estado miembro de conformidad con el presente Reglamento sólo sea posible cuando y en la medida en que el Estado miembro de que se trate haya decidido prever expresamente la posibilidad de autorizar dicho uso en sus disposiciones de Derecho interno. Por consiguiente, los Estados miembros siguen siendo libres, en virtud del presente Reglamento, de no prever dicha posibilidad en absoluto o de preverla únicamente con respecto a algunos de los objetivos que pueden justificar una utilización autorizada identificados en el presente Reglamento. ***Dichas normas nacionales deben notificarse a la Comisión en un plazo de 30 días a partir de su adopción.***

(38) El uso de sistemas de IA para la identificación biométrica remota en tiempo real de personas físicas en espacios de acceso público con fines policiales implica necesariamente el tratamiento de datos biométricos. Las normas del presente Reglamento que prohíben, salvo determinadas excepciones, dicho uso, que se basan en el artículo 16 del TFUE, deben aplicarse como *lex specialis* respecto de las normas sobre el tratamiento de datos biométricos contenidas en el artículo 10 de la Directiva (UE) 2016/680, regulando así de manera exhaustiva dicho uso y el tratamiento de los datos biométricos implicados. Por consiguiente, dicho uso y tratamiento solo deben ser posibles en la medida en que sean compatibles con el marco establecido por el presente Reglamento, sin que exista margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines policiales, utilicen dichos sistemas y traten dichos datos en relación con ellos por los motivos enumerados en el artículo 10 de la Directiva (UE) 2016/680. En ese contexto, el presente Reglamento no tiene por objeto proporcionar la base jurídica para el tratamiento de datos personales con arreglo al artículo 8 de la Directiva (UE) 2016/680. No obstante, el uso de sistemas de identificación biométrica a distancia en tiempo real en espacios de acceso público con fines distintos de los policiales, incluso por parte de las autoridades competentes, no debe estar cubierto por el marco específico relativo a dicho uso con fines policiales establecido por el presente Reglamento. Por consiguiente, dicho uso para fines distintos de la aplicación de la ley no debe estar sujeto al requisito de una autorización con arreglo al presente Reglamento y a las normas detalladas aplicables del Derecho nacional que puedan dar efecto a dicha autorización.

(39) Todo tratamiento de datos biométricos y otros datos personales que conlleve el uso de sistemas de IA para la identificación biométrica, que no esté relacionado con el uso de sistemas de identificación biométrica a distancia en tiempo real en espacios de acceso público con fines policiales, tal como se regula en el presente Reglamento, ***debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. Para*** fines distintos de la aplicación de la ley, ▌ el artículo 9, apartado 1, del Reglamento (UE) 2016/679 ***y el*** artículo 10, apartado 1, del Reglamento (UE) 2018/1725 ***prohíben el tratamiento de datos biométricos, sin perjuicio de las excepciones limitadas previstas en dichos artículos. En la aplicación del*** artículo 9, ***apartado 1, del Reglamento (UE) 2016/679, el uso de la identificación biométrica a distancia para fines distintos de la aplicación de la ley ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos***.

(40) De conformidad con el artículo 6 bis del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al TUE y al TFUE, Irlanda no está vinculada por las normas establecidas en ***el artículo 5, apartado 1, letra c), en la medida en que se apliquen a la utilización de sistemas de categorización biométrica para actividades en el ámbito de la cooperación policial y judicial en materia penal, y en el artículo 5, apartado 1, letras e) y f), en la medida en que se apliquen a la utilización de sistemas de IA cubiertos por dicha disposición,*** el artículo 5, ***apartados 3 a 8, y el artículo 26, apartado 10,*** del presente Reglamento adoptado sobre la base del artículo 16 del TFUE, que se refieren al tratamiento de datos personales por los Estados miembros al llevar a cabo actividades incluidas en el ámbito de aplicación del capítulo 4 o del capítulo 5 del título V de la tercera parte del TFUE, cuando Irlanda no esté vinculada por las normas que regulan las formas de cooperación judicial en materia penal o de cooperación policial que exigen el cumplimiento de las disposiciones establecidas sobre la base del artículo 16 del TFUE.

(41) De conformidad con los artículos 2 y 2 bis del Protocolo n.o 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no está vinculada por las normas establecidas en el artículo ***5, apartado 1, letra c), en la medida en que se aplica a la utilización de sistemas de clasificación biométrica para actividades en el ámbito de la cooperación policial y judicial en materia penal, el artículo 5, apartado 1, letra e), la letra f), en la medida en que se aplique a la utilización de los sistemas de IA contemplados en dicha disposición, el artículo*** 5, ***apartados 3 a 8, y el artículo 26, apartado 10,*** del presente Reglamento adoptado sobre la base del artículo 16 del TFUE, o a reserva de su aplicación, que se refieran al tratamiento de datos personales por los Estados miembros en el ejercicio de actividades comprendidas en el ámbito de aplicación del capítulo 4 o del capítulo 5 del título V de la tercera parte del TFUE.

(42) ***En consonancia con la presunción de inocencia, las personas físicas de la Unión deben ser juzgadas siempre por su comportamiento real. Las personas físicas nunca deben ser juzgadas por un comportamiento previsto por la IA basado únicamente en su perfil, rasgos de personalidad o características, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de automóvil, sin una sospecha razonable de que esa persona esté implicada en una actividad delictiva basada en hechos objetivos verificables y sin una evaluación humana de la misma. Por lo tanto, deben prohibirse las evaluaciones de riesgo realizadas en relación con personas físicas con el fin de evaluar el riesgo de que delincan o de predecir la comisión de una infracción penal real o potencial basándose únicamente en la elaboración de perfiles o en la evaluación de sus rasgos y características de personalidad. En cualquier caso, dicha prohibición no se refiere ni afecta a los análisis de riesgos que no se basan en la elaboración de perfiles de personas físicas o en los rasgos y características de su personalidad, como los sistemas de IA que utilizan análisis de riesgos para evaluar el riesgo de fraude financiero de las empresas sobre la base de transacciones sospechosas o las herramientas de análisis de riesgos para predecir la probabilidad de localización de estupefacientes o mercancías ilícitas por parte de las autoridades aduaneras, por ejemplo sobre la base de rutas de tráfico conocidas.***

(43) ***La comercialización, la puesta en servicio con este fin específico o el uso de sistemas de inteligencia artificial que creen o amplíen bases de datos de reconocimiento facial mediante el rastreo no selectivo de imágenes faciales de Internet o de grabaciones de CCTV deben prohibirse porque esta práctica aumenta la sensación de vigilancia masiva y puede dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad.***

(44) Existen serias dudas sobre la base científica de los sistemas de IA que pretenden identificar o inferir emociones, sobre todo porque la expresión de las emociones varía considerablemente entre culturas y situaciones, e incluso dentro de un mismo individuo. Entre las principales deficiencias de estos sistemas se encuentran su escasa fiabilidad, su falta de especificidad y su limitada generalizabilidad. Por lo tanto, los sistemas de IA que identifican o infieren emociones o intenciones de las personas físicas sobre la base de sus datos biométricos pueden dar lugar a resultados discriminatorios y pueden ser intrusivos para los derechos y libertades de las personas afectadas. Teniendo en cuenta el desequilibrio de poder en el contexto del trabajo o la educación, combinado con la naturaleza intrusiva de estos sistemas, tales sistemas podrían conducir a un trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros de ellas. Por consiguiente, debe prohibirse la comercialización, la puesta en servicio o el uso de sistemas de IA destinados a ser utilizados para detectar el estado emocional de las personas en situaciones relacionadas con el trabajo y la educación. Esta prohibición no debe aplicarse a los sistemas de IA comercializados por razones estrictamente médicas o de seguridad, como los sistemas destinados a uso terapéutico.

(45) Las prácticas prohibidas por la legislación de la Unión, incluida la legislación sobre protección de datos, no discriminación, protección de los consumidores y competencia, no deben verse afectadas por el presente Reglamento.

(46) Los sistemas de IA de alto riesgo solo deben introducirse en el mercado de la Unión**,** ponerse en servicio ***o utilizarse*** si cumplen determinados requisitos obligatorios. Estos requisitos deben garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuyos resultados se utilicen de otro modo en la Unión no planteen riesgos inaceptables para los intereses públicos importantes de la Unión reconocidos y protegidos por el Derecho de la Unión. Sobre la ***base del nuevo marco legislativo, tal como se aclara en la Comunicación de la Comisión titulada "Guía azul para la aplicación de las normas de la UE sobre productos de 2022"[21], la norma general es que la legislación de armonización de la Unión, como los Reglamentos (UE) [2017/74522] y (UE) [2017/74623] del Parlamento Europeo y del Consejo y la Directiva 2006/42/CE del Parlamento Europeo y del [Consejo24], puede ser aplicable a un producto, ya que la puesta a disposición o la puesta en servicio solo puede tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Para garantizar la coherencia y evitar una carga administrativa innecesaria o costes innecesarios, los proveedores de un producto que contenga uno o más sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento o de la legislación de armonización de la Unión enumerada en un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas sobre cómo garantizar la conformidad de un producto que contenga uno o más sistemas de IA con todos los requisitos aplicables de la legislación de armonización de la Unión de manera óptima.*** Los sistemas de IA identificados como de alto riesgo deben limitarse a aquellos que tengan un impacto perjudicial significativo en la salud, la seguridad y los derechos fundamentales de las personas en la Unión y dicha limitación minimice cualquier posible restricción al comercio internacional.

---

21 ***DO C 247 de 29.6.2022, p. 1.***

22 Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

23 Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios para diagnóstico *in vitro* y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

[24] Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24).

(47) Los sistemas de IA podrían ***tener repercusiones*** negativas para la salud y la seguridad de las personas, en particular cuando dichos sistemas funcionan como componentes de seguridad. En consonancia con los objetivos de la legislación de armonización de la Unión de facilitar la libre circulación de productos en el mercado interior y de garantizar que solo los productos seguros y conformes en otros aspectos lleguen al mercado, es importante que los riesgos para la seguridad que pueda generar un producto en su conjunto debido a sus componentes digitales, incluidos los sistemas de IA, se prevengan y mitiguen debidamente. Por ejemplo, los robots cada vez más autónomos, ya sea en el contexto de la fabricación o de la asistencia y los cuidados personales, deben ser capaces de operar con seguridad y desempeñar sus funciones en entornos complejos. Del mismo modo, en el sector sanitario, donde lo que está en juego es especialmente la vida y la salud, los sistemas de diagnóstico cada vez más sofisticados y los sistemas de apoyo a las decisiones humanas deben ser fiables y precisos. ▌

(48) ***El alcance del impacto adverso causado por el sistema de IA sobre los derechos fundamentales protegidos por la Carta es de especial relevancia a la hora de clasificar un sistema de IA como de alto riesgo. Estos derechos incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos personales, la libertad de expresión e información, la libertad de reunión y de asociación, y la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas con discapacidad, la igualdad de género, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, el derecho de defensa y la presunción de inocencia, el derecho a una buena administración. Además de estos derechos, es importante destacar que los niños tienen derechos específicos consagrados en el artículo 24 de la Carta y en la Convención de las Naciones Unidas sobre los Derechos del Niño, desarrollados en la Observación General nº 25 de la Convención de las Naciones Unidas sobre los Derechos del Niño en lo que respecta al entorno digital, que exigen que se tengan en cuenta las vulnerabilidades de los niños y que se les proporcione la protección y los cuidados necesarios para su bienestar. El derecho fundamental a un alto nivel de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión también debe tenerse en cuenta al evaluar la gravedad del daño que puede causar un sistema de IA, incluso en relación con la salud y la seguridad de las personas.***

(49) Por lo que respecta a los sistemas de IA de alto riesgo que son componentes de seguridad de productos o sistemas, o que son en sí mismos productos o sistemas incluidos en el ámbito de aplicación del Reglamento (CE) nº 300/2008 del Parlamento Europeo y del **Consejo25**, el Reglamento (UE) nº 167/2013 del Parlamento Europeo y del **Consejo26**, Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del **Consejo27,** Directiva 2014/90/UE del Parlamento Europeo y del **Consejo28**, Directiva (UE) 2016/797 del Parlamento Europeo y del **Consejo29**, Reglamento (UE) 2018/858 del Parlamento Europeo y del **Consejo30**,

---

25 Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) nº 2320/2002 (DO L 97 de 9.4.2008, p. 72).

26 Reglamento (UE) nº 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos agrícolas y forestales (DO L 60 de 2.3.2013, p. 1).

27 Reglamento (UE) nº 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos de dos o tres ruedas y los cuatriciclos (DO L 60 de 2.3.2013, p. 52).

28 Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos y por la que se deroga la Directiva 96/98/CE del Consejo (DO L 257 de 28.8.2014, p. 146).

29 Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea (DO L 138 de 26.5.2016, p. 44).

30 Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1).

Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo[31], y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo[32], procede modificar dichos actos para garantizar que la Comisión tenga en cuenta, sobre la base de las especificidades técnicas y reglamentarias de cada sector, y sin interferir con los mecanismos y autoridades de gobernanza, evaluación de la conformidad y ejecución existentes establecidos en ellos, los requisitos obligatorios para los sistemas de IA de alto riesgo establecidos en el presente Reglamento al adoptar cualquier acto delegado o de ejecución pertinente sobre la base de dichos actos.

---

31 Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea y se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010, (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1).

32 Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, sobre los requisitos de homologación de tipo de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, en lo relativo a su seguridad general y a la protección de los ocupantes de vehículos y usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.o 78/2009, (CE) n.o 79/2009 y (CE) n.o 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n.o 631/2009, (UE) n.o 406/2010, (UE) n.o 672/2010, (UE) n.o 1003/2010, (UE) n.o 1005/2010, (UE) n.o 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012 y (UE) 2015/166 (DO L 325 de 16.12.2019, p. 1).

(50) Por lo que respecta a los sistemas de IA que son componentes de seguridad de productos, o que son en sí mismos productos, que entran en el ámbito de aplicación de determinada legislación de armonización de la Unión, procede clasificarlos como de alto riesgo con arreglo al presente Reglamento si el producto en cuestión se somete al procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros con arreglo a dicha legislación de armonización de la Unión pertinente. En particular, tales productos son las máquinas, los juguetes, los ascensores, los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas, los equipos radioeléctricos, los equipos a presión, los equipos para embarcaciones de recreo, las instalaciones de transporte por cable, los aparatos de gas, los productos sanitarios y los productos sanitarios para diagnóstico *in vitro*.

(51) La clasificación de un sistema de IA como de alto riesgo con arreglo al presente Reglamento no debe significar necesariamente que el producto cuyo componente de seguridad sea el sistema de IA, o el propio sistema de IA como producto, se considere de alto riesgo con arreglo a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto. Este es, en particular, el caso de los Reglamentos (UE) 2017/745 y (UE) 2017/746, en los que se prevé una evaluación de la conformidad por terceros para los productos de riesgo medio y alto.

(52) Por lo que respecta a los sistemas de IA independientes, es decir, los sistemas de IA de alto riesgo distintos de los que son componentes de seguridad, o que son en sí mismos productos, procede clasificarlos como de alto riesgo si, a la luz de su finalidad prevista, plantean un alto riesgo de daño para la salud y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible daño como su probabilidad de ocurrencia, y se utilizan en una serie de ámbitos predefinidos específicamente que se especifican en el presente Reglamento. La identificación de dichos sistemas se basa en la misma metodología y criterios previstos también para cualquier modificación futura de la lista de sistemas de IA de alto riesgo ***que la Comisión debe estar facultada para adoptar, mediante actos delegados, para tener en cuenta el rápido ritmo del desarrollo tecnológico, así como los posibles cambios en el uso de los sistemas de IA***.

(53) También es importante aclarar que puede haber casos específicos en los que los sistemas de IA referidos a ámbitos predefinidos especificados en el presente Reglamento no conlleven un riesgo significativo de perjuicio de los intereses jurídicos protegidos en dichos ámbitos porque no influyan materialmente en la toma de decisiones o no perjudiquen sustancialmente dichos intereses. A efectos del presente Reglamento, un sistema de IA que no influye materialmente en el resultado de la toma de decisiones debe entenderse como un sistema de IA que no tiene un impacto en la sustancia, y por tanto en el resultado, de la toma de decisiones, ya sea humana o automatizada. Un sistema de IA que no influye materialmente en el resultado de la toma de decisiones podría incluir situaciones en las que se cumplen una o más de las siguientes condiciones. La primera de estas condiciones debe ser que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada, como un sistema de IA que transforme datos no estructurados en datos estructurados, un sistema de IA que clasifique documentos entrantes en categorías o un sistema de IA que se utilice para detectar duplicados entre un gran número de aplicaciones. Estas tareas son de naturaleza tan estrecha y limitada que sólo plantean riesgos limitados que no aumentan por el uso en un contexto que figura como uso de alto riesgo en un anexo del presente Reglamento. La segunda condición debe ser que la tarea realizada por el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada que pueda ser pertinente a efectos de dicha lista. Teniendo en cuenta estas características, el sistema de IA sólo proporciona una capa adicional a una actividad humana con el consiguiente menor riesgo. Esta condición se aplicaría, por ejemplo, a los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos previamente redactados, por ejemplo en relación con el tono profesional, el estilo académico del lenguaje o alineando el texto con un determinado mensaje de marca.

La tercera condición debe ser que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores. El riesgo se reduciría porque el uso del sistema de IA sigue a una evaluación humana previamente realizada, a la que no pretende sustituir ni influir, sin una revisión humana adecuada. Estos sistemas de IA incluyen, por ejemplo, los que, dado un determinado patrón de calificación de un profesor, pueden utilizarse para comprobar a posteriori si el profesor puede haberse desviado del patrón de calificación, con el fin de señalar posibles incoherencias o anomalías. La cuarta condición debe ser que el sistema de IA esté destinado a realizar una tarea que sólo sea preparatoria de una evaluación pertinente a efectos de los sistemas de IA enumerados en un anexo del presente Reglamento, con lo que el posible impacto del resultado del sistema será muy bajo en términos de representar un riesgo para la evaluación posterior. Esta condición abarca, entre otros, las soluciones inteligentes para el tratamiento de archivos, que incluyen diversas funciones de indexación, búsqueda, tratamiento de texto y voz o vinculación de datos a otras fuentes de datos, o los sistemas de IA utilizados para la traducción de documentos iniciales. En cualquier caso, debe considerarse que esos sistemas de IA de alto riesgo plantean riesgos significativos de perjuicio para la salud, la seguridad o los derechos fundamentales de las personas físicas si el sistema de IA implica la elaboración de perfiles en el sentido del artículo 4, punto 4, del Reglamento (UE) 2016/679 o del artículo 3, punto 4, de la Directiva (UE) 2016/680 o del artículo 3, punto 5, del Reglamento (UE) 2018/1725. Para garantizar la trazabilidad y la transparencia, un proveedor que considere que un sistema de IA no es de alto riesgo sobre la base de esas condiciones debe elaborar la documentación de la evaluación antes de que dicho sistema se comercialice o se ponga en servicio y debe facilitar esta documentación a las autoridades nacionales competentes a petición de estas. Dicho proveedor debe estar obligado a registrar el sistema en la base de datos de la UE creada en virtud del presente Reglamento. Con vistas a proporcionar orientaciones adicionales para la aplicación práctica de las condiciones en las que los sistemas de IA de alto riesgo enumerados en el anexo son, con carácter excepcional, de no alto riesgo, la Comisión, previa consulta al Consejo, debe proporcionar directrices que especifiquen dicha aplicación práctica completadas con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA de alto riesgo y de no alto riesgo.

▌

(54) ***Dado que los datos biométricos constituyen una categoría especial de datos personales sensibles, conviene clasificar como de alto riesgo varios casos de uso crítico de los sistemas biométricos, en la medida en que su uso esté permitido por el Derecho nacional y de la Unión pertinente. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica a distancia de personas físicas pueden dar lugar a resultados sesgados y conllevar efectos discriminatorios. El riesgo de tales resultados sesgados y efectos discriminatorios es especialmente relevante en relación con la edad, la etnia, la raza, el sexo o las discapacidades. Por lo tanto, los sistemas de identificación biométrica a distancia deben clasificarse como de alto riesgo en vista de los riesgos que plantean. Dicha clasificación excluye los sistemas de IA destinados a ser utilizados para la verificación biométrica, incluida la autenticación, cuyo único propósito es confirmar que una persona física específica es quien dice ser y confirmar la identidad de una persona física con el único propósito de tener acceso a un servicio, desbloquear un dispositivo o tener acceso seguro a locales. Además, los sistemas de IA destinados a ser utilizados para la categorización biométrica con arreglo a atributos o características sensibles protegidos en virtud del artículo 9, apartado 1, del Reglamento (UE) 2016/679 sobre la base de datos biométricos, en la medida en que no estén prohibidos en virtud del presente Reglamento, y los sistemas de reconocimiento de emociones que no estén prohibidos en virtud del presente Reglamento, deben clasificarse como de alto riesgo. No deben considerarse sistemas de alto riesgo los sistemas biométricos destinados a ser utilizados únicamente con el fin de habilitar medidas de ciberseguridad y protección de datos personales.***

(55) Por lo que respecta a la gestión y explotación de infraestructuras críticas, procede clasificar como de alto riesgo los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y explotación de ***infraestructuras digitales críticas enumeradas en el anexo I, punto (8),a la Directiva (UE) 2022/2557, el*** tráfico por carretera y el suministro de agua, gas, calefacción y electricidad, ya que su fallo o mal funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y provocar perturbaciones apreciables en el desarrollo ordinario de las actividades sociales y económicas. Los ***componentes de seguridad de las infraestructuras críticas, incluidas las infraestructuras digitales críticas, son sistemas utilizados para proteger directamente la integridad física de las infraestructuras críticas o la salud y la seguridad de las personas y los bienes, pero que no son necesarios para que el sistema funcione. El fallo o mal funcionamiento de dichos componentes podría provocar directamente riesgos para la integridad física de las infraestructuras críticas y, por tanto, riesgos para la salud y la seguridad de las personas y los bienes. Los componentes destinados a ser utilizados únicamente con fines de ciberseguridad no deben considerarse componentes de seguridad. Ejemplos de componentes de seguridad de tales infraestructuras críticas pueden ser los sistemas de control de la presión del agua o los sistemas de control de alarmas contra incendios en centros de computación en nube.***

(56) ***El despliegue de sistemas de IA en la educación es importante para promover una educación y formación digitales de alta calidad y para permitir que todos los alumnos y profesores adquieran y compartan las habilidades y competencias digitales necesarias, incluida la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos. Sin embargo, los sistemas de IA*** utilizados en la educación o la formación profesional, en particular para determinar el acceso o ***la admisión, para*** asignar a las personas a instituciones o ***programas*** educativos y de formación profesional ***en todos los niveles, para evaluar los resultados del aprendizaje de*** las personas***, para evaluar el nivel de educación adecuado para una persona e influir materialmente en el nivel de educación y formación que las personas recibirán o al que podrán acceder, o para supervisar y detectar comportamientos prohibidos de los estudiantes durante las pruebas,*** deben ***clasificarse como sistemas de IA de alto riesgo***, ya que pueden determinar el curso educativo y profesional de la vida de una persona y, por lo tanto, afectar a su capacidad para asegurarse un medio de vida. Cuando se diseñan y utilizan de forma inadecuada, estos sistemas ***pueden ser especialmente intrusivos y*** vulnerar el derecho a la educación y a la formación, así como el derecho a no ser discriminado, y perpetuar pautas históricas de discriminación***, por ejemplo contra las mujeres, determinados grupos de edad, personas con discapacidad o personas de determinados orígenes raciales o étnicos u orientación sexual***.

(57) Los sistemas de IA utilizados en el empleo, la gestión de trabajadores y el acceso al trabajo por cuenta propia, en particular para la contratación y la selección de personas, para la toma de decisiones ***que afectan a las condiciones de la relación laboral,*** la promoción y la finalización ***de las relaciones contractuales laborales, para la asignación de tareas sobre la base del comportamiento individual, los rasgos o las características personales y para el*** seguimiento o la evaluación de las personas en relaciones contractuales laborales, también deben clasificarse como de alto riesgo, ya que dichos sistemas pueden tener un impacto apreciable en las perspectivas futuras de carrera***, los*** medios de subsistencia de dichas personas ***y los derechos de los trabajadores***. Las relaciones contractuales pertinentes relacionadas con el trabajo deben implicar, de ***manera significativa,*** a los trabajadores y a las personas que prestan servicios a través de plataformas, tal como se contempla en el Programa de Trabajo de la Comisión para 2021. A lo largo del proceso de contratación y en la evaluación, promoción o retención de personas en relaciones contractuales relacionadas con el trabajo, dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, personas con discapacidad o personas de determinados orígenes raciales o étnicos u orientación sexual. Los sistemas de IA utilizados para controlar el rendimiento y el comportamiento de dichas personas también pueden ***menoscabar*** sus derechos fundamentales a la protección de datos y a la intimidad.

(58) Otro ámbito en el que el uso de los sistemas de IA merece una consideración especial es el acceso y disfrute de determinados servicios y prestaciones privados y públicos esenciales necesarios para que las personas participen plenamente en la sociedad o mejoren su nivel de vida. En particular, ▌ las personas físicas que solicitan ***o reciben prestaciones y servicios esenciales de asistencia pública de las autoridades públicas, a saber,*** servicios de ***asistencia sanitaria, prestaciones de la seguridad social,*** servicios sociales ***que proporcionan protección en casos tales como maternidad, enfermedad, accidentes laborales, dependencia o vejez y pérdida del empleo y*** ayudas ***sociales y para la vivienda,*** suelen depender de dichas prestaciones y servicios y se encuentran en una posición vulnerable en relación con las autoridades responsables. Si se utilizan sistemas de IA para determinar si las autoridades deben ***conceder,*** denegar, reducir, revocar o reclamar dichas prestaciones y servicios, ***incluso si los beneficiarios tienen derecho legítimo a tales prestaciones o servicios, dichos sistemas*** pueden tener un impacto significativo en los medios de subsistencia de las personas y vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a un recurso efectivo, por lo que deben clasificarse como de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y la utilización de enfoques innovadores en la administración pública, que podría beneficiarse de un uso más amplio de sistemas de IA conformes y seguros, siempre que dichos sistemas no entrañen un riesgo elevado para las personas físicas y jurídicas.

Además, los sistemas de IA utilizados para evaluar la puntuación crediticia o la solvencia de las personas físicas deben clasificarse como sistemas de IA de alto riesgo, ya que determinan el acceso de esas personas a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA utilizados para esos fines pueden dar lugar a discriminación entre personas o grupos y perpetuar pautas históricas de discriminación, como la basada en el origen racial o étnico, el sexo, la discapacidad, la edad o la orientación sexual, o crear nuevas formas de impacto discriminatorio. No obstante, los sistemas de IA previstos por el Derecho de la Unión con fines de detección del fraude en la oferta de servicios financieros y con fines prudenciales para calcular los requisitos de capital de las entidades de crédito y las empresas de seguros no deben considerarse de alto riesgo con arreglo al presente Reglamento. Por otra parte, los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas para los seguros de salud y de vida también pueden tener un impacto significativo en los medios de vida de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y acarrear graves consecuencias para la vida y la salud de las personas, incluida la exclusión financiera y la discriminación. Por último, los sistemas de IA utilizados para ***evaluar y clasificar las llamadas de emergencia de personas físicas o para*** despachar o establecer la prioridad en el despacho de los servicios de primera respuesta de emergencia***, incluidos los de policía, bomberos y ayuda médica, así como de los sistemas de triaje de pacientes de asistencia sanitaria de emergencia,*** también deben clasificarse como de alto riesgo, ya que toman decisiones en situaciones muy críticas para la vida y la salud de las personas y sus bienes.

(59) ***Habida cuenta de su función y responsabilidad,*** las actuaciones de las fuerzas y cuerpos de seguridad que implican determinados usos de los sistemas de IA se caracterizan por un importante grado de desequilibrio de poder y pueden dar lugar a la vigilancia, detención o privación de libertad de una persona física, así como a otras repercusiones negativas sobre los derechos fundamentales garantizados en la Carta. En particular, si el sistema de IA no se entrena con datos de alta calidad, no cumple los requisitos adecuados en cuanto a su ***rendimiento, su*** precisión o solidez, o no se diseña y prueba adecuadamente antes de su comercialización o puesta en servicio de otro modo, puede señalar a personas de forma discriminatoria o de otro modo incorrecto o injusto. Además, el ejercicio de importantes derechos fundamentales procesales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como el derecho de defensa y la presunción de inocencia, podría verse obstaculizado, en particular, cuando tales sistemas de IA no sean suficientemente transparentes, explicables y documentados. Por lo tanto, procede clasificar como de alto riesgo***, en la medida en que su uso esté permitido por el Derecho de la Unión y nacional pertinente,*** una serie de sistemas de IA destinados a ser utilizados en el contexto policial, en el que la precisión, la fiabilidad y la transparencia son especialmente importantes para evitar repercusiones negativas, conservar la confianza pública y garantizar la rendición de cuentas y la reparación efectiva.

Habida cuenta de la naturaleza de las actividades y de los riesgos conexos, estos sistemas de IA de alto riesgo deben incluir, en particular, los sistemas de IA destinados a ser utilizados por las autoridades policiales ***o los órganos, oficinas o agencias de la Unión, o en su nombre, en apoyo de las autoridades policiales, para evaluar el riesgo de que una persona*** física sea ***víctima de infracciones penales, como polígrafos y herramientas similares, para la evaluación de la*** fiabilidad de las pruebas en el curso de la investigación o ***el enjuiciamiento de infracciones*** penales ***y, en la medida en que no esté prohibido en virtud del presente Reglamento, para evaluar el riesgo de que una persona física delinca o reincida no basándose únicamente en la*** elaboración de perfiles de personas físicas ***o en la evaluación de*** rasgos y características de la personalidad o del comportamiento delictivo anterior de personas físicas o grupos, para la elaboración de perfiles en el curso de la detección, investigación o enjuiciamiento de infracciones penales ▌ . Los sistemas de IA destinados específicamente a ser utilizados en procedimientos administrativos por las autoridades fiscales y aduaneras, ***así como por las unidades de inteligencia financiera que lleven a cabo tareas administrativas de análisis de la información con arreglo a la legislación de la Unión contra el blanqueo de capitales,*** no deben ***clasificarse como*** sistemas de IA de alto riesgo utilizados por las fuerzas y cuerpos de seguridad con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales. ***El uso de herramientas de IA por parte de las fuerzas y cuerpos de seguridad y las autoridades no debe convertirse en un factor de desigualdad o exclusión. No deben ignorarse las repercusiones del uso de herramientas de IA en los derechos de defensa de los sospechosos, en particular la dificultad de obtener información significativa sobre el funcionamiento de esos sistemas y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas físicas investigadas.***

(60) Los sistemas de IA utilizados en la gestión de la migración, el asilo y el control de fronteras afectan a personas que a menudo se encuentran en una situación especialmente vulnerable y que dependen del resultado de las actuaciones de las autoridades públicas competentes. La exactitud, el carácter no discriminatorio y la transparencia de los sistemas de IA utilizados en esos contextos son, por tanto, especialmente importantes para garantizar el respeto de los derechos fundamentales de las personas afectadas, en particular sus derechos a la libre circulación, a la no discriminación, a la protección de la vida privada y de los datos personales, a la protección internacional y a una buena administración. Por consiguiente, procede clasificar como de alto riesgo***, en la medida en que su uso esté permitido en virtud del Derecho de la Unión y nacional pertinente, los*** sistemas de IA destinados a ser utilizados por las autoridades públicas competentes ***o por las instituciones, órganos u organismos de la Unión*** encargados de tareas en los ámbitos de la gestión de la migración, el asilo y el control de fronteras, ***o en su nombre,*** como polígrafos e instrumentos similares***,*** para evaluar determinados riesgos que presentan las personas físicas que entran en el territorio de un Estado miembro o solicitan visado o asilo***,*** para asistir a las autoridades públicas competentes en el examen***, incluida la correspondiente evaluación de la fiabilidad de las pruebas, de*** las solicitudes de asilo, visado y permisos de residencia y las reclamaciones conexas con el objetivo de determinar la admisibilidad de las personas físicas que solicitan un estatuto***, a efectos de detectar, reconocer o identificar a personas físicas en el contexto de la gestión de la migración, el asilo y el control fronterizo, con excepción de la verificación de los documentos de viaje***.

Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo cubiertos por el presente Reglamento deben cumplir los requisitos de procedimiento pertinentes establecidos por el Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del **Consejo33**, la Directiva 2013/32/UE del Parlamento Europeo y del **Consejo34** y demás legislación pertinente de la Unión. El ***uso de sistemas de IA en la gestión de la migración, el asilo y el control de fronteras no debe, en ningún caso, ser utilizado por los Estados miembros o las instituciones, órganos u organismos de la Unión como medio para eludir sus obligaciones internacionales en virtud de la Convención de las Naciones Unidas sobre el Estatuto de los Refugiados, hecha en Ginebra el 28 de julio de 1951 y modificada por el Protocolo de 31 de enero de 1967. Tampoco deben utilizarse para infringir en modo alguno el principio de no devolución, ni para denegar vías legales seguras y efectivas de entrada en el territorio de la Unión, incluido el derecho a la protección internacional.***

33 ▌ Reglamento (CE) nº 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre Visados (Código de visados) (DO L 243 de 15.9.2009, p. 1).

34 ▌ Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para conceder o retirar la protección internacional (DO L

180 de 29.6.2013, p. 60).

(61) Determinados sistemas de IA destinados a la administración de justicia y a los procesos democráticos deben clasificarse como de alto riesgo, teniendo en cuenta su impacto potencialmente significativo en la democracia, el Estado de Derecho, las libertades individuales, así como el derecho a un recurso efectivo y a un juicio justo. En particular, para hacer frente a los riesgos de posibles sesgos, errores y opacidad, conviene calificar de alto riesgo los sistemas de IA destinados a ***ser utilizados por una autoridad judicial o en su nombre para*** asistir a las autoridades judiciales en la investigación e interpretación de los hechos y de la ley y en la aplicación de la ley a un conjunto concreto de hechos. ***Los sistemas de IA destinados a ser utilizados por los órganos de resolución alternativa de litigios para estos fines también deben considerarse de alto riesgo cuando los resultados de los procedimientos de resolución alternativa de litigios produzcan efectos jurídicos para las partes. El uso de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe sustituirlo: la toma de decisiones final debe seguir siendo una actividad humana.*** No obstante, ***la clasificación de los sistemas de IA como de alto riesgo*** no debe extenderse a los sistemas de IA destinados a actividades administrativas puramente auxiliares que no afecten a la administración real de justicia en casos concretos, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre el personal, las tareas administrativas ▌.

(62) Sin perjuicio de las normas previstas en el Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo35+, y para hacer frente a los riesgos de injerencia externa indebida en el derecho de voto consagrado en el artículo 39 de la Carta, y de efectos adversos en la democracia y el Estado de Derecho, los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos deben clasificarse como sistemas de IA de alto riesgo, con excepción de los sistemas de IA a cuyos resultados no están expuestas directamente las personas físicas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico.

(63) El hecho de que un sistema de IA esté clasificado como ***sistema de IA*** de alto riesgo con arreglo al presente Reglamento no debe interpretarse como una indicación de que el uso del sistema es ▌ lícito en virtud de otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión, como los relativos a la protección de datos personales, al uso de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Cualquier uso de este tipo debe seguir produciéndose únicamente de conformidad con los requisitos aplicables derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho nacional. No debe entenderse que el presente Reglamento establece el fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, cuando proceda***, a menos que el presente Reglamento disponga específicamente lo contrario***.

---

35 Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., sobre la transparencia y la orientación de la publicidad política (DO L, ..., ELI: ...).

+ DO: por favor, inserte en el texto el número del Reglamento en PE 90/23 (2021/0381(COD)) y complete la nota a pie de página correspondiente.

(64) Para mitigar los riesgos de los sistemas de IA de alto riesgo comercializados ***o*** puestos en servicio ***y garantizar un alto nivel de fiabilidad***, deben aplicarse determinados requisitos obligatorios ***a los sistemas de IA de alto riesgo***, teniendo en cuenta la finalidad prevista ***y el contexto de*** uso del sistema de ***IA*** y de acuerdo con el sistema de gestión de riesgos que establezca el proveedor. ***Las medidas adoptadas por los proveedores para cumplir los requisitos obligatorios del presente Reglamento deben tener en cuenta el estado de la técnica generalmente reconocido en materia de IA, ser proporcionadas y eficaces para cumplir los objetivos del presente Reglamento. Sobre la base del nuevo marco legislativo, tal como se aclara en la Comunicación de la Comisión "Guía azul sobre la aplicación de las normas de la UE relativas a los productos de 2022", la norma general es que la legislación de armonización de la Unión puede ser aplicable a un producto, ya que la puesta a disposición o puesta en servicio sólo puede tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Los peligros de los sistemas de IA cubiertos por los requisitos del presente Reglamento se refieren a aspectos diferentes de los de los actos de armonización de la Unión existentes y, por tanto, los requisitos del presente Reglamento complementarían el corpus existente de actos de armonización de la Unión. Por ejemplo, los productos de maquinaria o productos sanitarios que incorporen un sistema de IA podrían presentar riesgos no abordados por los requisitos esenciales de salud y seguridad establecidos en la legislación armonizada de la Unión pertinente, ya que dicha legislación sectorial no se ocupa de los riesgos específicos de los sistemas de IA.***

Esto exige una aplicación simultánea y complementaria de los distintos actos legislativos. Para garantizar la coherencia y evitar una carga administrativa innecesaria y costes innecesarios, los proveedores de un producto que contenga uno o más sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento y de la legislación de armonización de la Unión basada en el nuevo marco legislativo enumerada en un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas sobre cómo garantizar el cumplimiento de un producto que contenga uno o más sistemas de IA con todos los requisitos aplicables de dicha legislación armonizada de la Unión de manera óptima. Esa flexibilidad podría significar, por ejemplo, la decisión del proveedor de integrar una parte de los procesos necesarios de ensayo y notificación, información y documentación exigidos en virtud del presente Reglamento en la documentación y los procedimientos ya existentes exigidos en virtud de la legislación de armonización de la Unión vigente basada en el nuevo marco legislativo enumerado en un anexo del presente Reglamento. Ello no menoscabará en modo alguno la obligación del proveedor de cumplir todos los requisitos aplicables.

(65) ***El sistema de gestión de riesgos debe consistir en un proceso continuo e iterativo que se planifique y ejecute a lo largo de todo el ciclo de vida de un sistema de IA de alto riesgo. Este proceso debe tener por objeto identificar y mitigar los riesgos pertinentes de los sistemas de IA para la salud, la seguridad y los derechos fundamentales. El sistema de gestión de riesgos debe revisarse y actualizarse periódicamente para garantizar su eficacia permanente, así como la justificación y documentación de todas las decisiones y medidas significativas adoptadas con arreglo al presente Reglamento. Este proceso debe garantizar que el proveedor identifique los riesgos o impactos adversos y aplique medidas de mitigación de los riesgos conocidos y razonablemente previsibles de los sistemas de IA para la salud, la seguridad y los derechos fundamentales a la luz de su finalidad prevista y del mal uso razonablemente previsible, incluidos los posibles riesgos derivados de la interacción entre el sistema de IA y el entorno en el que opera. El sistema de gestión de riesgos debe adoptar las medidas de gestión de riesgos más adecuadas a la luz del estado de la técnica en materia de IA. A la hora de identificar las medidas de gestión de riesgos más adecuadas, el proveedor debe documentar y explicar las opciones elegidas y, cuando proceda, implicar a expertos y partes interesadas externas. Al determinar el uso indebido razonablemente previsible de los sistemas de IA de alto riesgo, el proveedor deberá abarcar los usos de los sistemas de IA que, aunque no estén directamente cubiertos por la finalidad prevista y contemplados en las instrucciones de uso, pueda esperarse razonablemente que resulten de un comportamiento humano fácilmente previsible en el contexto de las características específicas y del uso de un sistema de IA concreto.***

Cualquier circunstancia conocida o previsible relacionada con el uso del sistema de IA de alto riesgo de acuerdo con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales, deberá incluirse en las instrucciones de uso facilitadas por el proveedor. Con ello se pretende garantizar que el usuario las conozca y las tenga en cuenta al utilizar el sistema de IA de alto riesgo.

La identificación y aplicación de medidas de mitigación de riesgos para usos indebidos previsibles con arreglo al presente Reglamento no debe exigir medidas específicas de formación adicional para el sistema de IA de alto riesgo por parte del proveedor para abordarlas. No obstante, se anima a los proveedores a considerar tales medidas de formación adicionales para mitigar los usos indebidos razonablemente previsibles, según sea necesario y adecuado.

(66) Deben aplicarse requisitos a los sistemas de IA de alto riesgo en lo que respecta a la ***gestión de riesgos,*** la calidad ***y pertinencia*** de los conjuntos de datos utilizados, la documentación técnica y el mantenimiento de registros, la transparencia y el suministro de información a ***los usuarios***, la supervisión humana, y la solidez, exactitud y ciberseguridad. Estos requisitos son necesarios para mitigar eficazmente los riesgos para la salud, la seguridad y los derechos fundamentales, ▌ y no se dispone razonablemente de otras medidas menos restrictivas del comercio, evitando así restricciones injustificadas al comercio.

(67) ***Los datos de alta calidad y el acceso a datos*** de alta calidad ***desempeñan un papel vital a la hora de proporcionar estructura y garantizar*** el rendimiento de muchos sistemas de IA, especialmente cuando se utilizan técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione según lo previsto y de forma segura y no se convierta en ***una*** fuente de discriminación prohibida por el Derecho de la Unión. Los conjuntos de datos de alta calidad para el entrenamiento, la validación y las ***pruebas requieren la aplicación de prácticas adecuadas de gobernanza y gestión de datos. Los conjuntos de datos para la formación, la validación y las pruebas, incluidas las etiquetas, deben ser pertinentes, suficientemente representativos y, en la medida de lo posible,*** libres de errores y completos a la vista de la finalidad prevista del sistema. ***Para facilitar el cumplimiento de la legislación de la Unión en materia de protección de datos, como el Reglamento (UE) 2016/679, las prácticas de gobernanza y gestión de datos deben incluir, en el caso de los datos personales, la transparencia sobre la finalidad original de la recogida de datos. Los conjuntos de datos*** también deben tener las propiedades estadísticas adecuadas, incluso en lo que respecta a las personas o grupos de personas ***en relación con los cuales se*** pretende utilizar el sistema de IA de alto riesgo***, con especial atención a la mitigación de posibles sesgos en los conjuntos de datos, que puedan afectar a la salud y la seguridad de las personas, tener un impacto negativo en los derechos fundamentales o dar lugar a discriminaciones prohibidas por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las entradas para futuras operaciones (bucles de retroalimentación). Los sesgos pueden, por ejemplo, ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generarse cuando los sistemas se aplican en entornos del mundo real.***

Los resultados proporcionados por los sistemas de IA podrían verse influidos por estos sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, a perpetuar y amplificar la discriminación existente, en particular para las personas vulnerables pertenecientes a determinados grupos, incluidos los grupos raciales o étnicos. El requisito de que los conjuntos de datos sean, en la medida de lo posible, completos y estén libres de errores no debe afectar al uso de técnicas que preserven la intimidad en el contexto del desarrollo y las pruebas de los sistemas de IA. En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos propios del entorno geográfico, ***contextual,*** conductual o funcional específico en el que se pretende utilizar el sistema de IA. ***Los requisitos relativos a la gobernanza de los datos pueden cumplirse recurriendo a terceros que ofrezcan servicios certificados de conformidad, incluida la verificación de la gobernanza de los datos, la integridad de los conjuntos de datos y las prácticas de formación, validación y ensayo de datos, en la medida en que se garantice el cumplimiento de los requisitos relativos a los datos del presente Reglamento.***

(68) Para el desarrollo ***y la evaluación*** de los sistemas de IA de alto riesgo, determinados agentes, como los proveedores, los organismos notificados y otras entidades pertinentes, como los Centros Europeos de Innovación Digital, las instalaciones de experimentación y los investigadores, deben poder acceder a conjuntos de datos de alta calidad y utilizarlos en los ámbitos de actividad de dichos agentes relacionados con el presente Reglamento. Los espacios comunes europeos de datos establecidos por la Comisión y la facilitación de la puesta en común de datos entre empresas y con las administraciones públicas en aras del interés público serán fundamentales para proporcionar un acceso fiable, responsable y no discriminatorio a datos de alta calidad para la formación, validación y ensayo de sistemas de IA. Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a los datos sanitarios y la formación de algoritmos de IA en esos conjuntos de datos, de una manera que preserve la privacidad, segura, oportuna, transparente y fiable, y con una gobernanza institucional adecuada. Las autoridades competentes pertinentes, incluidas las sectoriales, que faciliten o apoyen el acceso a los datos también podrán apoyar el suministro de datos de alta calidad para el entrenamiento, la validación y el ensayo de los sistemas de IA.

(69) El derecho a la intimidad y a la protección de los datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en la legislación de la Unión sobre protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de dichos principios pueden incluir no solo la anonimización y el cifrado, sino también el uso de tecnología que permita llevar algoritmos a los datos y permita el entrenamiento de los sistemas de IA sin la transmisión entre las partes o la copia de los propios datos en bruto o estructurados, sin perjuicio de los requisitos sobre gobernanza de datos previstos en el presente Reglamento.

(70) Con el fin de proteger el derecho de los demás frente a la discriminación que podría derivarse del sesgo en los sistemas de IA, los proveedores deben, excepcionalmente, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de sesgos en relación con los sistemas de IA de alto riesgo, con sujeción a las salvaguardias adecuadas de los derechos y libertades fundamentales de las personas físicas y tras la aplicación de todas las condiciones aplicables establecidas en virtud del presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y en la Directiva (UE) 2016/680, poder tratar también categorías especiales de datos personales, como una cuestión de interés público importante en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, punto (g) del Reglamento (UE) 2018/1725.

(71) Disponer de información ***comprensible*** sobre cómo se han desarrollado los sistemas de IA de alto riesgo y cómo funcionan a lo largo de su ***vida útil*** es esencial para ***permitir la trazabilidad de dichos sistemas,*** verificar el cumplimiento de los requisitos del presente Reglamento***, así como el seguimiento de sus operaciones y la supervisión posterior a la comercialización***. Para ello es necesario mantener registros y disponer de una documentación técnica que contenga la información necesaria para evaluar la conformidad del sistema de IA con los requisitos pertinentes ***y facilitar el seguimiento posterior a la comercialización***. Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema, los algoritmos, los datos, la formación, las pruebas y los procesos de validación utilizados, así como la documentación sobre el sistema de gestión de riesgos pertinente ***y elaborada de forma clara y completa.*** La documentación técnica debe mantenerse actualizada***, de forma adecuada, durante toda la vida útil del sistema de IA***. ***Además, los sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de eventos, mediante registros, durante toda la vida útil del sistema.***

(72) Para abordar ***las preocupaciones relacionadas con la*** opacidad ***y la complejidad de*** determinados sistemas de IA ***y ayudar a los implantadores a cumplir sus obligaciones en virtud del presente Reglamento,*** debe exigirse transparencia a los sistemas de IA de alto riesgo ***antes de su comercialización o puesta en servicio. Los sistemas de IA de alto riesgo*** deben ***diseñarse de manera que los implantadores puedan entender cómo funciona el*** sistema de ***IA, evaluar su funcionalidad y comprender sus puntos fuertes y sus limitaciones. Los sistemas de*** IA de alto ***riesgo*** deben ir acompañados de la ***información adecuada en forma de*** instrucciones de uso***. Dicha información debe*** incluir ***las características, capacidades y limitaciones de funcionamiento del sistema de IA. Dichos elementos abarcarían*** información ***sobre las posibles circunstancias conocidas o previsibles relacionadas con el uso del sistema de IA de alto riesgo***, incluida ***la actuación del desplegador que pueda influir en el comportamiento y el rendimiento del sistema, en las que el sistema de IA pueda dar lugar a*** riesgos para ***la salud, la seguridad y los*** derechos fundamentales***, sobre los cambios que hayan sido previamente determinados y evaluados para su conformidad por el proveedor y sobre las medidas pertinentes de supervisión humana, incluidas las medidas para facilitar la interpretación de los resultados del sistema de IA por parte de los desplegadores. La transparencia, incluidas las instrucciones de uso adjuntas, debe ayudar a los usuarios a utilizar el sistema y a tomar decisiones con conocimiento de causa. Entre otras cosas, los usuarios deben estar en mejores condiciones de elegir correctamente el sistema que pretenden utilizar a la luz de las obligaciones que les incumben, ser informados de los usos previstos y excluidos, y utilizar el sistema de IA correctamente y según proceda. Para mejorar la legibilidad y accesibilidad de la información incluida en las instrucciones de uso,*** cuando proceda, ***deben incluirse ejemplos ilustrativos, por ejemplo sobre las limitaciones y sobre los usos previstos y excluidos del sistema de IA. Los proveedores deben velar por que toda la documentación, incluidas las instrucciones de uso, contenga información significativa, completa, accesible y comprensible, teniendo en cuenta las necesidades y los conocimientos previsibles de los destinatarios del despliegue. Las instrucciones de uso deben estar disponibles en una lengua fácilmente comprensible para los destinatarios, según determine el Estado miembro de que se trate.***

(73) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de forma que las personas físicas puedan supervisar su funcionamiento***, garantizar que se utilizan según lo previsto y que sus impactos se abordan a lo largo del ciclo de vida del sistema***. Para ello, el proveedor del sistema deberá determinar las medidas de supervisión humana adecuadas antes de su comercialización o puesta en servicio. En particular, cuando proceda, dichas medidas deben garantizar que el sistema esté sujeto a restricciones operativas incorporadas que no puedan ser anuladas por el propio sistema y que responda al operador humano, y que las personas físicas a las que se haya asignado la supervisión humana tengan la competencia, la formación y la autoridad necesarias para desempeñar esa función. ***También es esencial, según proceda, garantizar que los sistemas de IA de alto riesgo incluyan mecanismos para guiar e informar a la persona física a la que se haya asignado la supervisión humana para que tome decisiones con conocimiento de causa sobre si debe intervenir, cuándo y cómo hacerlo para evitar consecuencias negativas o riesgos, o detener el sistema si no funciona según lo previsto. Teniendo en cuenta las importantes consecuencias para las personas en caso de coincidencia incorrecta por parte de determinados sistemas de identificación biométrica, conviene establecer un requisito reforzado de supervisión humana para dichos sistemas, de modo que el responsable de la aplicación no pueda adoptar ninguna medida o decisión sobre la base de la identificación resultante del sistema a menos que ésta haya sido verificada y confirmada por separado por al menos dos personas físicas. Dichas personas podrán pertenecer a una o varias entidades e incluir a la persona que opere o utilice el sistema. Este requisito no debería suponer una carga o un retraso innecesarios y podría bastar con que las verificaciones por separado de las distintas personas se registraran automáticamente en los registros generados por el sistema. Dadas las especificidades de los ámbitos de la aplicación de la ley, la migración, el control de fronteras y el asilo, este requisito no debe aplicarse cuando el Derecho de la Unión o nacional considere desproporcionada la aplicación de dicho requisito.***

(74) Los sistemas de IA de alto riesgo deben funcionar de forma coherente a lo largo de su ciclo de vida y alcanzar un nivel adecuado de precisión, solidez y ciberseguridad***, a la luz de su finalidad prevista y de conformidad con el*** estado de la técnica generalmente reconocido. ***Se anima a la Comisión y a las organizaciones y partes interesadas pertinentes a que tengan debidamente en cuenta la mitigación de los riesgos y las repercusiones negativas del sistema de IA. El*** nivel ***esperado de las métricas de rendimiento debe declararse en las instrucciones de uso adjuntas. Se insta a los proveedores a comunicar esa información a los usuarios de forma clara y fácilmente comprensible, sin malentendidos ni declaraciones engañosas. El Derecho de la Unión en materia de metrología legal, incluidas las Directivas 2014/31/UE[36] y 2014/32/UE[37] del Parlamento Europeo y del Consejo, tiene por objeto garantizar la exactitud de las mediciones y contribuir a la transparencia y equidad de las transacciones comerciales. En ese contexto, en cooperación con las partes interesadas y las organizaciones pertinentes, como las autoridades de metrología y evaluación comparativa, la Comisión debe fomentar, según proceda, el desarrollo de parámetros de referencia y metodologías de medición para los sistemas de IA. Para ello, la Comisión debería tomar nota y colaborar con los socios internacionales que trabajan en metrología e indicadores de medición pertinentes relacionados con la IA.***

---

36 Directiva 2014/31/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros relativas a la comercialización de instrumentos de pesaje de funcionamiento no automático (DO L 96 de 29.3.2014, p. 107).

37 Directiva 2014/32/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de instrumentos de medida (DO L 096 de 29.3.2014, p. 149).

(75) La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo. Deben ser resistentes en ***relación con los comportamientos nocivos o indeseables que puedan derivarse de las*** limitaciones ***de los sistemas o del entorno en el que funcionan*** (por ejemplo, errores, fallos, incoherencias, situaciones inesperadas)***. Por lo tanto, deben adoptarse medidas técnicas y organizativas para garantizar la solidez de los sistemas de IA de alto riesgo, por ejemplo diseñando y desarrollando soluciones técnicas adecuadas para prevenir o minimizar los comportamientos nocivos o indeseables***. ***Estas soluciones técnicas pueden incluir, por ejemplo, mecanismos que permitan al sistema interrumpir su funcionamiento de forma segura (planes a prueba de fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de ciertos límites predeterminados. La*** falta de protección contra estos riesgos podría tener repercusiones en la seguridad o afectar negativamente a los derechos fundamentales, por ejemplo debido a decisiones erróneas o resultados equivocados o sesgados generados por el sistema de IA.

(76) La ciberseguridad desempeña un papel crucial a la hora de garantizar que los sistemas de IA sean resistentes a los intentos de alterar su uso, comportamiento y rendimiento, o de comprometer sus propiedades de seguridad por parte de terceros malintencionados que exploten las vulnerabilidades del sistema. Los ciberataques contra los sistemas de IA pueden aprovechar activos específicos de la IA, como conjuntos de datos de entrenamiento (por ejemplo, envenenamiento de datos) o modelos entrenados (por ejemplo, ataques de adversarios ***o inferencia de miembros***), o explotar vulnerabilidades en los activos digitales del sistema de IA o en la infraestructura de TIC subyacente. Para garantizar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas***, como controles de seguridad, teniendo*** también en cuenta, según proceda, la infraestructura de TIC subyacente.

(77) ***Sin perjuicio de los requisitos relativos a la robustez y precisión establecidos en el presente Reglamento, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo38+, de conformidad con el artículo 8 de dicho Reglamento, podrán demostrar el cumplimiento de los requisitos de ciberseguridad del presente Reglamento mediante el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el artículo 10 y en el anexo I del Reglamento (UE) 2024/...++.Cuando los sistemas de IA de alto riesgo cumplan los requisitos esenciales del Reglamento (UE) 2024/...++, deben considerarse conformes con los requisitos de ciberseguridad establecidos en el presente Reglamento en la medida en que la consecución de dichos requisitos se demuestre en la declaración UE de conformidad o en partes de la misma expedida con arreglo al Reglamento (UE) 2024/...++. A tal fin, la evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales clasificados como sistema de inteligencia artificial de alto riesgo con arreglo al presente Reglamento, realizada en virtud del Reglamento (UE) nº 2024/...++, debe tener en cuenta los riesgos para la resistencia cibernética de un sistema de inteligencia artificial en lo que respecta a los intentos de terceros no autorizados de alterar su uso, comportamiento o rendimiento, incluidas las vulnerabilidades específicas de la inteligencia artificial, como el envenenamiento de datos o los ataques de adversarios, así como, en su caso, los riesgos para los derechos fundamentales exigidos por el presente Reglamento.***

---

38 Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., sobre los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020 (DO L, ..., ELI: ...).

+ DO: por favor, inserte en el texto el número del Reglamento en PE XX/YY (2022/0272(COD)) y complete la nota a pie de página correspondiente.

(78) El procedimiento de evaluación de la conformidad previsto en el presente Reglamento debe aplicarse en relación con los requisitos esenciales de ciberseguridad de un producto con elementos digitales cubierto por el Reglamento (UE) 2024/...[+] y clasificado como sistema de IA de alto riesgo con arreglo al presente Reglamento. No obstante, esta norma no debe dar lugar a una reducción del nivel de garantía necesario para los productos críticos con elementos digitales cubiertos por el Reglamento (UE) 2024/...[+]. Por consiguiente, no obstante lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entran en el ámbito de aplicación del presente Reglamento y que también están calificados como productos importantes y críticos con elementos digitales con arreglo al Reglamento (UE) 2024/...[+] y a los que se aplica el procedimiento de evaluación de la conformidad basado en el control interno establecido en un anexo del presente Reglamento, están sujetos a las disposiciones de evaluación de la conformidad del Reglamento (UE) 2024/...[+] en lo que respecta a los requisitos esenciales de ciberseguridad de dicho Reglamento. En este caso, para todos los demás aspectos cubiertos por el presente Reglamento deben aplicarse las disposiciones respectivas sobre evaluación de la conformidad basada en el control interno establecidas en un anexo del presente Reglamento. Basándose en los conocimientos y la experiencia de la ENISA sobre la política de ciberseguridad y las tareas asignadas a la ENISA en virtud del Reglamento (UE) 2019/1020, la Comisión debe cooperar con la ENISA en cuestiones relacionadas con la ciberseguridad de los sistemas de IA.

+ DO: por favor, inserte el número del Reglamento en PE XX/YY (2022/0272(COD)).

()

(79) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad de la comercialización o puesta en servicio de un sistema de IA de alto riesgo, con independencia de que dicha persona física o jurídica sea la que haya diseñado o desarrollado el sistema.

(80) Como signatarios de la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad, la Unión y los Estados miembros están jurídicamente obligados a proteger a las personas con discapacidad contra la discriminación y a promover su igualdad, a velar por que las personas con discapacidad tengan acceso, en igualdad de condiciones con las demás, a las tecnologías y sistemas de la información y las comunicaciones, y a garantizar el respeto de la intimidad de las personas con discapacidad. Dada la creciente importancia y uso de los sistemas de IA, la aplicación de los principios de diseño universal a todas las nuevas tecnologías y servicios debe garantizar el acceso pleno y en igualdad de condiciones de todas las personas potencialmente afectadas por las tecnologías de IA o que las utilicen, incluidas las personas con discapacidad, de forma que se tenga plenamente en cuenta su dignidad y diversidad inherentes. Por lo tanto, es esencial que los proveedores garanticen el pleno cumplimiento de los requisitos de accesibilidad, incluida la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo[39] y la Directiva (UE) 2019/882. Los proveedores deben garantizar el cumplimiento de estos requisitos mediante el diseño. Por lo tanto, las medidas necesarias deben integrarse en la medida de lo posible en el diseño del sistema de IA de alto riesgo.

[39] Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016,

relativa a la accesibilidad de los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público (DO L 327 de 2.12.2016, p. 1).

(81) El proveedor debe establecer un sistema de gestión de la calidad sólido, garantizar la realización del procedimiento de evaluación de la conformidad requerido, elaborar la documentación pertinente y establecer un sistema sólido de seguimiento poscomercialización. Los proveedores ***de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad en virtud de la legislación sectorial pertinente de la Unión deben tener la posibilidad de incluir los elementos del sistema de gestión de la calidad previstos en el presente Reglamento como parte del sistema de gestión de la calidad existente previsto en esa otra legislación sectorial de la Unión. La complementariedad entre el presente Reglamento y el Derecho sectorial de la Unión vigente también debe tenerse en cuenta en las futuras actividades de normalización u orientaciones que adopte la Comisión.*** Las autoridades públicas que pongan en servicio sistemas de IA de alto riesgo para su propio uso podrán adoptar y aplicar las normas del sistema de gestión de la calidad como parte del sistema de gestión de la calidad adoptado a nivel nacional o regional, según proceda, teniendo en cuenta las especificidades del sector y las competencias y la organización de la autoridad pública de que se trate.

(82) Para permitir la aplicación del presente Reglamento y crear condiciones de igualdad para los operadores, y teniendo en cuenta las diferentes formas de puesta a disposición de los productos digitales, es importante garantizar que, en cualquier circunstancia, una persona establecida en la Unión pueda facilitar a las autoridades toda la información necesaria sobre la conformidad de un sistema de IA. Por consiguiente, antes de poner a disposición sus sistemas de IA en la Unión, ▌ los proveedores establecidos en terceros países designarán, mediante mandato escrito, a un representante autorizado establecido en la Unión. ***Este representante autorizado desempeña un papel fundamental a la hora de garantizar la conformidad de los sistemas de IA de alto riesgo comercializados o puestos en servicio en la Unión por aquellos proveedores que no estén establecidos en la Unión y de actuar como su persona de contacto establecida en la Unión.***

(83) Habida cuenta de la naturaleza y la complejidad de la cadena de valor de los sistemas de IA y en consonancia con el nuevo marco legislativo, es esencial garantizar la seguridad jurídica y facilitar el cumplimiento del presente Reglamento. Por lo tanto, es necesario aclarar el papel y las obligaciones específicas de los operadores pertinentes a lo largo de la cadena de valor, como los importadores y distribuidores que pueden contribuir al desarrollo de los sistemas de IA. En determinadas situaciones, esos operadores podrían actuar en más de una función al mismo tiempo y, por lo tanto, deberían cumplir acumulativamente todas las obligaciones pertinentes asociadas a esas funciones. Por ejemplo, un operador podría actuar como distribuidor e importador al mismo tiempo.

(84) ***Para garantizar la seguridad jurídica, es necesario aclarar que, en determinadas condiciones*** específicas***, cualquier distribuidor, importador, implantador u otro tercero debe ser considerado proveedor de un sistema de IA de alto riesgo y, por tanto, asumir todas las*** obligaciones ***pertinentes. Este sería el caso si dicha parte pone su nombre o marca comercial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo, o si dicha parte realiza una modificación sustancial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio de forma que siga siendo un sistema de IA de alto riesgo de conformidad con el presente Reglamento, o si modifica la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido clasificado como de alto riesgo y que ya haya sido comercializado o puesto en servicio, de manera que el sistema de IA se convierta en un sistema de IA de alto riesgo de conformidad con el presente Reglamento. Dichas disposiciones deben aplicarse sin perjuicio de disposiciones más específicas establecidas en determinada legislación de armonización de la Unión basada en el nuevo marco legislativo, junto con las cuales debe aplicarse el presente Reglamento. Por ejemplo, el artículo 16, apartado 2, del Reglamento (UE) 2017/745, que establece que determinados cambios no*** deben considerarse ***modificaciones de un producto que puedan afectar a su conformidad con los requisitos aplicables, debe seguir aplicándose a los sistemas de IA de alto riesgo que sean productos sanitarios en el sentido de dicho Reglamento***.

(85) ***Los sistemas de IA de propósito general pueden utilizarse como sistemas de IA de alto riesgo por sí mismos o ser componentes de otros sistemas de IA de alto riesgo. Por lo tanto, debido a su naturaleza particular y con el fin de garantizar un reparto equitativo de responsabilidades a lo largo de la cadena de valor de la IA, los proveedores de dichos sistemas deben, con independencia de si pueden ser utilizados como sistemas de IA de alto riesgo como tales por otros proveedores o como componentes de sistemas de IA de alto riesgo y salvo disposición en contrario en virtud del presente Reglamento, cooperar estrechamente con los proveedores de los sistemas de IA de alto riesgo pertinentes para permitirles cumplir las obligaciones pertinentes en virtud del presente Reglamento y con las autoridades competentes establecidas en virtud del presente Reglamento.***

(86) ***Cuando, en las condiciones establecidas en el presente Reglamento, el proveedor que inicialmente comercializó o puso en servicio el sistema de IA deje de ser considerado el proveedor a efectos del presente Reglamento, y cuando dicho proveedor no haya excluido expresamente la transformación del sistema de IA en un sistema de IA de alto riesgo, el antiguo proveedor deberá, no obstante, cooperar estrechamente y facilitar la información necesaria y proporcionar el acceso técnico y demás asistencia que razonablemente se prevea que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo.***

(87) Además, cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto que entre en el ámbito de aplicación de la legislación de armonización de la Unión basada en el nuevo marco legislativo no se comercialice ni se ponga en servicio independientemente del producto, el fabricante del producto definido en dicha legislación debe cumplir las obligaciones del proveedor establecidas en el presente Reglamento y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumple los requisitos del presente Reglamento.

(88) A lo largo de la cadena de valor de la IA, múltiples partes suministran a menudo sistemas, herramientas y servicios de IA, pero también componentes o procesos que son incorporados por el proveedor al sistema de IA con diversos objetivos, entre ellos el entrenamiento de modelos, el reentrenamiento de modelos, la prueba y evaluación de modelos, la integración en programas informáticos u otros aspectos del desarrollo de modelos. Dichas partes tienen un papel importante que desempeñar en la cadena de valor con respecto al proveedor del sistema de IA de alto riesgo en el que se integran sus sistemas, herramientas, servicios, componentes o procesos de IA, y deben proporcionar a este proveedor, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y demás asistencia necesarios basados en el estado de la técnica generalmente reconocido, con el fin de que el proveedor pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento, sin comprometer sus propios derechos de propiedad intelectual o secretos comerciales.

(89) ***Los terceros que pongan a disposición del público herramientas, servicios, procesos o componentes de la IA distintos de los modelos de IA de propósito general no estarán obligados a cumplir los requisitos relativos a las responsabilidades a lo largo de la cadena de valor de la IA, en particular con respecto al proveedor que los haya utilizado o integrado, cuando dichas herramientas, servicios, procesos o componentes de la IA se pongan a disposición del público con una licencia libre y abierta. Debe animarse a los desarrolladores de herramientas, servicios, procesos o componentes de IA gratuitos y de código abierto distintos de los modelos de IA de uso general a que apliquen prácticas de documentación ampliamente adoptadas, como tarjetas de modelo y fichas de datos, como forma de acelerar el intercambio de información a lo largo de la cadena de valor de la IA, permitiendo la promoción de sistemas de IA fiables en la Unión.***

(90) ***La Comisión podría desarrollar y recomendar cláusulas contractuales tipo voluntarias entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en sistemas de IA de alto riesgo, para facilitar la cooperación a lo largo de la cadena de valor. Al desarrollar modelos de cláusulas contractuales voluntarias, la Comisión también debería tener en cuenta los posibles requisitos contractuales aplicables en sectores o casos empresariales específicos.***

(91) Habida cuenta de la naturaleza de los sistemas de IA y de los riesgos para la seguridad y los derechos fundamentales que puede conllevar su utilización, incluida la necesidad de garantizar una supervisión adecuada del funcionamiento de un sistema de IA en un entorno real, conviene establecer responsabilidades específicas para los responsables del despliegue**.** En particular, los ***responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que*** utilizan los sistemas de IA de alto riesgo de conformidad con las instrucciones de uso, y deben establecerse otras obligaciones en relación con la supervisión del funcionamiento de los sistemas de IA y con el mantenimiento de registros, según proceda. ***Además, los responsables del despliegue deben garantizar que las personas asignadas para aplicar las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan la competencia necesaria, en particular un nivel adecuado de conocimientos de IA, formación y autoridad para desempeñar correctamente esas tareas. Estas obligaciones deben entenderse sin perjuicio de otras obligaciones de los responsables del despliegue en relación con los sistemas de IA de alto riesgo en virtud del Derecho de la Unión o nacional.***

(92) El presente Reglamento se entiende sin perjuicio de las obligaciones de los empresarios de informar o de informar y consultar a los trabajadores o a sus representantes en virtud del Derecho y las prácticas de la Unión o nacionales, incluida la Directiva 2002/14/CE del Parlamento Europeo y del Consejo[40] relativa a un marco general relativo a la información y a la consulta de los trabajadores sobre las decisiones de puesta en servicio o de utilización de los sistemas de IA. Sigue siendo necesario garantizar la información de los trabajadores y sus representantes sobre el despliegue previsto de sistemas de IA de alto riesgo en el lugar de trabajo cuando no se cumplan las condiciones para dicha información o las obligaciones de información y consulta previstas en otros instrumentos jurídicos. Además, tal derecho de información es accesorio y necesario para el objetivo de protección de los derechos fundamentales que subyace en el presente Reglamento. Por consiguiente, debe establecerse en el presente Reglamento un requisito de información a tal efecto, sin que ello afecte a ninguno de los derechos existentes de los trabajadores.

---

40 Directiva 2002/14/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 2002, por la que se establece un marco general relativo a la información y a la consulta de los

trabajadores en la Comunidad Europea - Declaración conjunta del Parlamento Europeo, del Consejo y de la Comisión relativa a la representación de los trabajadores (DO L 80 de 23.3.2002, p. 29).

(93) ***Si bien los riesgos relacionados con los sistemas de IA pueden derivarse de la forma en que se diseñan dichos sistemas, también pueden derivarse de la forma en que se utilizan. Por lo tanto, los implantadores de sistemas de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, complementando las obligaciones del proveedor al desarrollar el sistema de IA. Los encargados del despliegue son los más indicados para comprender cómo se utilizará concretamente el sistema de IA de alto riesgo y, por lo tanto, pueden identificar posibles riesgos significativos que no se hayan previsto en la fase de desarrollo, gracias a un conocimiento más preciso del contexto de uso y de las personas o grupos de personas que pueden verse afectados, incluidos los grupos de personas vulnerables. Los responsables del despliegue de los sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento también desempeñan un papel fundamental en la información a las personas físicas y deben, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, en su caso, informar a las personas físicas de que están sujetas al uso del sistema de IA de alto riesgo. Esta información deberá incluir la finalidad prevista y el tipo de decisiones que adopta. El implantador también debe informar a la persona física de su derecho a recibir una explicación con arreglo al presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo utilizados con fines policiales, dicha obligación debe aplicarse de conformidad con el artículo 13 de la Directiva (UE) 2016/680.***

(94) Todo tratamiento de datos biométricos relacionado con el uso de sistemas de IA para la identificación biométrica con fines policiales debe cumplir lo dispuesto en el artículo 10 de la Directiva (UE) 2016/680, que permite dicho tratamiento únicamente cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado, y cuando esté autorizado por el Derecho de la Unión o de los Estados miembros. Dicho uso, cuando esté autorizado, también debe respetar los principios establecidos en el artículo 4, apartado 1, de la Directiva (UE) 2016/680, incluidos la licitud, la equidad y la transparencia, la limitación de la finalidad, la exactitud y la limitación del almacenamiento.

(95) Sin perjuicio del Derecho de la Unión aplicable, en particular el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, considerando la naturaleza intrusiva de los sistemas de identificación biométrica a distancia, el uso de sistemas de identificación biométrica a distancia estará sujeto a salvaguardias. Los sistemas de identificación biométrica a distancia deben utilizarse siempre de forma proporcionada, legítima y estrictamente necesaria, y por tanto selectiva, en cuanto a las personas a identificar, la ubicación, el ámbito temporal y sobre la base de un conjunto cerrado de datos de secuencias de vídeo legalmente adquiridas. En cualquier caso, los sistemas de identificación biométrica a distancia no deben utilizarse en el marco de la aplicación de la ley para llevar a una vigilancia indiscriminada. En cualquier caso, las condiciones para la identificación biométrica a distancia no deben servir de base para eludir las condiciones de prohibición y las excepciones estrictas para la identificación biométrica a distancia en tiempo real.

(96) ***Con el fin de garantizar eficazmente la protección de los derechos fundamentales, quienes desplieguen sistemas de IA de alto riesgo que sean organismos de Derecho público, u operadores privados que presten servicios públicos y operadores que desplieguen determinados sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, como entidades bancarias o de seguros, deben llevar a cabo una evaluación de impacto sobre los derechos fundamentales antes de ponerlo en funcionamiento. Los servicios importantes para las personas que son de carácter público también pueden ser prestados por entidades privadas. Los operadores privados que prestan estos servicios de carácter público están vinculados a tareas de interés público, como en el ámbito de la educación, la asistencia sanitaria, los servicios sociales, la vivienda o la administración de justicia. El objetivo de la evaluación de impacto sobre los derechos fundamentales es que el implantador identifique los riesgos específicos para los derechos de las personas o grupos de personas que puedan verse afectados e identifique las medidas que deben adoptarse en caso de que se materialicen dichos riesgos. La evaluación de impacto debe aplicarse al primer uso del sistema de IA de alto riesgo, y debe actualizarse cuando el implantador considere que ha cambiado alguno de los factores pertinentes. La evaluación de impacto debe identificar los procesos pertinentes del implantador en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista, y debe incluir una descripción del período de tiempo y la frecuencia en que se prevé utilizar el sistema, así como de las categorías específicas de personas físicas y grupos que puedan verse afectados en el contexto específico de utilización.***

La evaluación también debe incluir la identificación de riesgos específicos de daños que puedan tener un impacto en los derechos fundamentales de esas personas o grupos. Al realizar esta evaluación, el responsable del despliegue debe tener en cuenta la información pertinente para una evaluación adecuada del impacto, incluida, entre otras, la información facilitada por el proveedor del sistema de IA de alto riesgo en las instrucciones de uso. A la luz de los riesgos identificados, los responsables del despliegue deben determinar las medidas que deben adoptarse en caso de que se materialicen dichos riesgos, incluidas, por ejemplo, las disposiciones de gobernanza en ese contexto específico de uso, como las disposiciones para la supervisión humana con arreglo a las instrucciones de uso o los procedimientos de tramitación de reclamaciones y de recurso, ya que podrían contribuir a mitigar los riesgos para los derechos fundamentales en casos de uso concretos. Tras realizar esa evaluación de impacto, el implantador deberá notificarlo a la autoridad de vigilancia del mercado pertinente. Cuando proceda, para recopilar la información pertinente necesaria para realizar la evaluación de impacto, los implantadores de sistemas de IA de alto riesgo, en particular cuando los sistemas de IA se utilicen en el sector público, podrían implicar a las partes interesadas pertinentes, incluidos los representantes de los grupos de personas que puedan verse afectadas por el sistema de IA, expertos independientes y organizaciones de la sociedad civil, en la realización de dichas evaluaciones de impacto y en el diseño de las medidas que deban adoptarse en caso de que se materialicen los riesgos. La Oficina Europea de Inteligencia Artificial ("Oficina de IA") debería elaborar un modelo de cuestionario para facilitar el cumplimiento y reducir la carga administrativa de los implantadores.

(97) ***La noción de modelos de IA de propósito general debe definirse claramente y diferenciarse de la noción de sistemas de IA para permitir la seguridad jurídica. La definición debe basarse en las características funcionales clave de un modelo de IA de propósito general, en particular la generalidad y la capacidad de realizar de forma competente una amplia gama de tareas distintas. Estos modelos suelen entrenarse con grandes cantidades de datos, a través de diversos métodos, como el aprendizaje autosupervisado, no supervisado o de refuerzo. Los modelos de IA de propósito general pueden comercializarse de diversas formas, como a través de bibliotecas, interfaces de programación de aplicaciones (API), como descarga directa o como copia física. Estos modelos pueden modificarse o perfeccionarse para crear otros nuevos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen sistemas de IA por sí solos. Los modelos de IA requieren la adición de otros componentes, como por ejemplo una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen integrarse en los sistemas de IA y formar parte de ellos. El presente Reglamento establece normas específicas para los modelos de IA de propósito general y para los modelos de IA de propósito general que plantean riesgos sistémicos, que deben aplicarse también cuando estos modelos se integran o forman parte de un sistema de IA. Debe entenderse que las obligaciones para los proveedores de modelos de IA de propósito general deben aplicarse una vez que los modelos de IA de propósito general se comercializan.***

Cuando el proveedor de un modelo de IA de propósito general integra un modelo propio en su propio sistema de IA que se comercializa o se pone en servicio, debe considerarse que dicho modelo se comercializa y, por lo tanto, deben seguir aplicándose las obligaciones establecidas en el presente Reglamento para los modelos, además de las aplicables a los sistemas de IA. En cualquier caso, las obligaciones establecidas para los modelos no deben aplicarse cuando un modelo propio se utilice para procesos puramente internos que no sean esenciales para proporcionar un producto o un servicio a terceros y no se vean afectados los derechos de las personas físicas. Teniendo en cuenta sus posibles efectos significativamente negativos, los modelos de IA de propósito general con riesgo sistémico deben estar siempre sujetos a las obligaciones pertinentes en virtud del presente Reglamento. La definición no debe abarcar los modelos de IA utilizados antes de su comercialización con el único fin de realizar actividades de investigación, desarrollo y creación de prototipos. Ello se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando, tras dichas actividades, se comercialice un modelo.

(98) Mientras que la generalidad de un modelo podría, entre otros criterios, determinarse también por un número de parámetros, debería considerarse que los modelos con al menos mil millones de parámetros y entrenados con una gran cantidad de datos utilizando la autosupervisión a escala muestran una generalidad significativa y realizan de forma competente una amplia gama de tareas distintivas.

(99) Los grandes modelos generativos de IA son un ejemplo típico de modelo de IA de propósito general, dado que permiten generar contenidos de forma flexible, por ejemplo en forma de texto, audio, imágenes o vídeo, que pueden acomodarse fácilmente a una amplia gama de tareas distintivas.

(100) Cuando un modelo de IA de propósito general se integra en un sistema de IA o forma parte de él, este sistema debe considerarse un sistema de IA de propósito general cuando, debido a esta integración, este sistema tiene la capacidad de servir para diversos fines. Un sistema de IA de propósito general puede utilizarse directamente o puede integrarse en otros sistemas de IA.

(101) Los proveedores de modelos de IA de propósito general tienen un papel y una responsabilidad particulares a lo largo de la cadena de valor de la IA, ya que los modelos que proporcionan pueden constituir la base de una serie de sistemas posteriores, a menudo proporcionados por proveedores posteriores que necesitan una buena comprensión de los modelos y sus capacidades, tanto para permitir la integración de dichos modelos en sus productos como para cumplir sus obligaciones en virtud de esta u otras normativas. Por lo tanto, deben establecerse medidas de transparencia proporcionadas, incluida la elaboración y actualización de la documentación, y el suministro de información sobre el modelo de IA de propósito general para su uso por parte de los proveedores posteriores. El proveedor del modelo de IA de propósito general debe elaborar y mantener al día la documentación técnica para ponerla a disposición de la Oficina de IA y de las autoridades nacionales competentes que la soliciten. El conjunto mínimo de elementos que deben incluirse en dicha documentación debe establecerse en anexos al presente Reglamento. La Comisión debe estar facultada para modificar dichos anexos mediante actos delegados en función de la evolución de la tecnología.

(102) Los programas informáticos y los datos, incluidos los modelos, publicados bajo una licencia libre y de código abierto que permita compartirlos abiertamente y en la que los usuarios puedan acceder, utilizar, modificar y redistribuir libremente dichos programas o versiones modificadas de los mismos, pueden contribuir a la investigación y la innovación en el mercado y ofrecer importantes oportunidades de crecimiento para la economía de la Unión. Debe considerarse que los modelos de IA de propósito general publicados bajo licencias libres y de código abierto garantizan altos niveles de transparencia y apertura si sus parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo se ponen a disposición del público. También se considerará que la licencia es libre y de código abierto cuando permita a los usuarios ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software y los datos, incluidos los modelos, a condición de que se acredite al proveedor original del modelo y se respeten unas condiciones de distribución idénticas o comparables.

(103) Los componentes de IA libres y de código abierto abarcan el software y los datos, incluidos los modelos y los modelos de IA de propósito general, las herramientas, los servicios o los procesos de un sistema de IA. Los componentes de IA gratuitos y de código abierto pueden suministrarse a través de diferentes canales, incluido su desarrollo en repositorios abiertos. A efectos del presente Reglamento, los componentes de IA que se faciliten a cambio de un precio o se moneticen de otro modo, incluso mediante la prestación de asistencia técnica u otros servicios, incluso a través de una plataforma de software, relacionados con el componente de IA, o el uso de datos personales por razones distintas de la exclusiva mejora de la seguridad, compatibilidad o interoperabilidad del software, con la excepción de las transacciones entre microempresas, no deben beneficiarse de las excepciones previstas para los componentes de IA gratuitos y de fuente abierta. El hecho de poner a disposición componentes de IA a través de repositorios abiertos no debe constituir, en sí mismo, una monetización.

(104) Los proveedores de modelos de IA de propósito general que se publiquen con una licencia libre y de código abierto, y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, deben estar sujetos a excepciones por lo que respecta a los requisitos de transparencia impuestos a los modelos de IA de propósito general, a menos que pueda considerarse que presentan un riesgo sistémico, en cuyo caso la circunstancia de que el modelo sea transparente y vaya acompañado de una licencia de código abierto no debe considerarse razón suficiente para excluir el cumplimiento de las obligaciones previstas en el presente Reglamento. En cualquier caso, dado que la publicación de modelos de IA de propósito general con una licencia de código abierto no revela necesariamente información sustancial sobre el conjunto de datos utilizado para el entrenamiento o el ajuste del modelo y sobre cómo se ha garantizado con ello el cumplimiento de la legislación sobre derechos de autor, la excepción prevista para los modelos de IA de propósito general del cumplimiento de los requisitos relacionados con la transparencia no debe afectar a la obligación de elaborar un resumen sobre el contenido utilizado para el entrenamiento del modelo y la obligación de establecer una política para cumplir con la legislación de la Unión en materia de derechos de autor, en particular para identificar y cumplir con la reserva de derechos de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo[41].

41 Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019,

relativa a los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (DO L 130 de 17.5.2019, p. 92).

(105) Los modelos de propósito general, en particular los grandes modelos generativos, capaces de generar texto, imágenes y otros contenidos, presentan oportunidades únicas de innovación, pero también retos para los artistas, autores y otros creadores y la forma en que se crean, distribuyen, utilizan y consumen sus contenidos creativos. El desarrollo y entrenamiento de estos modelos requiere el acceso a grandes cantidades de texto, imágenes, vídeos y otros datos. Las técnicas de minería de textos y datos pueden utilizarse ampliamente en este contexto para la recuperación y el análisis de dichos contenidos, que pueden estar protegidos por derechos de autor y derechos afines. Cualquier uso de contenido protegido por derechos de autor requiere la autorización del titular de los derechos en cuestión, a menos que se apliquen las excepciones y limitaciones pertinentes de los derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras u otras materias, con fines de minería de textos y datos, en determinadas condiciones. En virtud de estas normas, los titulares de derechos pueden optar por reservar sus derechos sobre sus obras u otras materias para impedir la extracción de textos y datos, a menos que se haga con fines de investigación científica. Cuando los derechos de exclusión se hayan reservado expresamente de forma adecuada, los proveedores de modelos de IA de uso general deberán obtener una autorización de los titulares de los derechos si desean llevar a cabo minería de textos y datos sobre dichas obras.

(106) Los proveedores que comercialicen modelos de IA de propósito general en el mercado de la Unión deben garantizar el cumplimiento de las obligaciones pertinentes del presente Reglamento. A tal fin, los proveedores de modelos de IA de propósito general deben establecer una política de cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para identificar y cumplir las reservas de derechos expresadas por los titulares de derechos de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790. Cualquier proveedor que comercialice un modelo de IA de propósito general en el mercado de la Unión debe cumplir con esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos relevantes para los derechos de autor que sustentan la formación de esos modelos de IA de propósito general. Esto es necesario para garantizar la igualdad de condiciones entre los proveedores de modelos de IA de propósito general, donde ningún proveedor debe poder obtener una ventaja competitiva en el mercado de la Unión aplicando normas de derechos de autor inferiores a las previstas en la Unión.

(107) Con el fin de aumentar la transparencia sobre los datos que se utilizan en el preentrenamiento y el entrenamiento de los modelos de IA de propósito general, incluidos los textos y datos protegidos por la legislación sobre derechos de autor, es adecuado que los proveedores de dichos modelos elaboren y pongan a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de propósito general. Si bien debe tenerse debidamente en cuenta la necesidad de proteger los secretos comerciales y la información empresarial confidencial, este resumen debe ser generalmente exhaustivo en su alcance, en lugar de técnicamente detallado, para facilitar a las partes con intereses legítimos, incluidos los titulares de derechos de autor, el ejercicio y la aplicación de sus derechos en virtud del Derecho de la Unión, por ejemplo, enumerando las principales colecciones o conjuntos de datos que se utilizaron para entrenar el modelo, como grandes bases de datos privadas o públicas o archivos de datos, y proporcionando una explicación narrativa sobre otras fuentes de datos utilizadas. Conviene que la Oficina de AI facilite una plantilla para el resumen, que debe ser sencilla, eficaz y permitir al proveedor proporcionar el resumen requerido en forma narrativa.

(108) Por lo que respecta a las obligaciones impuestas a los proveedores de modelos de IA de propósito general de establecer una política de cumplimiento de la legislación de la Unión en materia de derechos de autor y poner a disposición del público un resumen del contenido utilizado para la formación, la Oficina de IA debe supervisar si el proveedor ha cumplido dichas obligaciones sin verificar ni proceder a una evaluación obra por obra de los datos de formación en términos de cumplimiento de los derechos de autor. El presente Reglamento no afecta a la aplicación de las normas sobre derechos de autor previstas en el Derecho de la Unión.

(109) ***El cumplimiento de las obligaciones aplicables a los proveedores de modelos de IA de propósito general debe ser proporcional y proporcionado al tipo de proveedor de modelos, excluyendo la necesidad de cumplimiento para las personas que desarrollen o utilicen modelos con fines no profesionales o de investigación científica, a las que, no obstante, debe animarse a cumplir voluntariamente estos requisitos. Sin perjuicio de la legislación de la Unión en materia de derechos de autor, el cumplimiento de estas obligaciones debe tener debidamente en cuenta el tamaño del proveedor y permitir formas simplificadas de cumplimiento para las PYME, incluidas las empresas de nueva creación, que no deben representar un coste excesivo ni desalentar el uso de dichos modelos. En caso de modificación o puesta a punto de un modelo, las obligaciones para los proveedores deben limitarse a dicha modificación o puesta a punto, por ejemplo complementando la documentación técnica ya existente con información sobre las modificaciones, incluidas las nuevas fuentes de datos de formación, como medio para cumplir las obligaciones de la cadena de valor previstas en el presente Reglamento.***

(110) ***Los modelos de IA de propósito general podrían plantear riesgos sistémicos que incluyen, entre otros, cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, interrupciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas; cualquier efecto negativo real o razonablemente previsible en los procesos democráticos, la seguridad pública y económica; la difusión de contenidos ilegales, falsos o discriminatorios. Debe entenderse que los riesgos sistémicos aumentan con las capacidades y el alcance del modelo, pueden surgir a lo largo de todo el ciclo de vida del modelo y se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la imparcialidad y la seguridad del modelo, el grado de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, estrategias de liberación y distribución, el potencial para eliminar barreras de protección y otros factores. En particular, los enfoques internacionales han señalado hasta ahora la necesidad de prestar atención a los riesgos derivados de un posible uso indebido intencionado o de problemas de control no intencionados relacionados con la alineación con la intención humana; los riesgos químicos, biológicos, radiológicos y nucleares, como las formas en que pueden reducirse las barreras de entrada, incluso para el desarrollo de armas, la adquisición de diseños o su uso; las capacidades cibernéticas ofensivas, como las formas en que puede permitirse el descubrimiento de vulnerabilidades, la explotación o el uso operativo; los efectos de la interacción y el uso de herramientas, incluida, por ejemplo, la capacidad de controlar sistemas físicos e interferir en infraestructuras críticas; los riesgos de que los modelos hagan copias de sí mismos o se "autorrepliquen" o entrenen a otros modelos; las formas en que los modelos pueden dar lugar a prejuicios y discriminaciones perjudiciales con riesgos para las personas, las comunidades o las sociedades; la facilitación de la desinformación o el daño a la privacidad con amenazas a los valores democráticos y los derechos humanos; el riesgo de que un acontecimiento concreto pueda dar lugar a una reacción en cadena con efectos negativos considerables que podrían afectar hasta a toda una ciudad, toda una actividad de dominio o toda una comunidad.***

(111) Conviene establecer una metodología para clasificar los modelos de IA de propósito general como modelos de IA de propósito general con riesgos sistémicos. Dado que los riesgos sistémicos se derivan de capacidades particularmente elevadas, debe considerarse que un modelo de IA de propósito general presenta riesgos sistémicos si tiene capacidades de alto impacto, evaluadas sobre la base de herramientas técnicas y metodologías adecuadas, o un impacto significativo en el mercado interior debido a su alcance. Por capacidades de alto impacto en los modelos de IA de propósito general se entienden capacidades que igualan o superan las capacidades registradas en los modelos de IA de propósito general más avanzados. La gama completa de capacidades de un modelo podría comprenderse mejor tras su lanzamiento al mercado o cuando los usuarios interactúen con el modelo. Según el estado de la técnica en el momento de la entrada en vigor del presente Reglamento, la cantidad acumulada de cálculo utilizada para el entrenamiento del modelo de IA de propósito general, medida en operaciones en coma flotante ("FLOPs"), es una de las aproximaciones pertinentes a las capacidades del modelo. La cantidad de cálculo utilizada para el entrenamiento acumula el cálculo utilizado en todas las actividades y métodos destinados a mejorar las capacidades del modelo antes de su despliegue, como el preentrenamiento, la generación de datos sintéticos y el ajuste fino. Por lo tanto, debe fijarse un umbral inicial de FLOPs que, si lo alcanza un modelo de IA de propósito general, lleve a presumir que se trata de un modelo de IA de propósito general con riesgos sistémicos. Este umbral debería ajustarse con el tiempo para reflejar los cambios tecnológicos e industriales, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, y debería complementarse con puntos de referencia e indicadores de la capacidad del modelo.

Para ello, la Oficina de Inteligencia Artificial debería colaborar con la comunidad científica, la industria, la sociedad civil y otros expertos. Los umbrales, así como las herramientas y los puntos de referencia para la evaluación de las capacidades de alto impacto, deberían ser sólidos predictores de la generalidad, sus capacidades y el riesgo sistémico asociado de los modelos de IA de propósito general, y podrían tener en cuenta la forma en que el modelo se comercializará o el número de usuarios a los que puede afectar. Para complementar este sistema, la Comisión debería tener la posibilidad de adoptar decisiones individuales por las que se designe un modelo de IA de propósito general como modelo de IA de propósito general con riesgo sistémico si se constata que dicho modelo tiene capacidades o un impacto equivalentes a los captados por el umbral establecido. Dicha decisión debe adoptarse sobre la base de una evaluación global de los criterios para la designación de modelos de IA de propósito general con riesgo sistémico establecidos en un anexo del presente Reglamento, como la calidad o el tamaño del conjunto de datos de entrenamiento, el número de empresas y usuarios finales, sus modalidades de entrada y salida, su grado de autonomía y escalabilidad, o las herramientas a las que tiene acceso. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de propósito general con riesgo sistémico, la Comisión debe tener en cuenta la solicitud y puede decidir reevaluar si puede seguir considerándose que el modelo de IA de propósito general presenta riesgos sistémicos.

(112) También es necesario aclarar un procedimiento para la clasificación de un modelo de IA de propósito general con riesgos sistémicos. Un modelo de IA de propósito general que alcance el umbral aplicable a las capacidades de alto impacto debe presumirse que es un modelo de IA de propósito general con riesgo sistémico. El proveedor deberá notificarlo a la Oficina de IA a más tardar dos semanas después de que se cumplan los requisitos o de que se tenga conocimiento de que un modelo de IA de propósito general cumplirá los requisitos que dan lugar a la presunción. Esto es especialmente relevante en relación con el umbral FLOP porque el entrenamiento de los modelos de IA de propósito general requiere una planificación considerable que incluye la asignación por adelantado de recursos informáticos y, por lo tanto, los proveedores de modelos de IA de propósito general pueden saber si su modelo cumpliría el umbral antes de que finalice el entrenamiento. En el contexto de esa notificación, el proveedor debe poder demostrar que, debido a sus características específicas, un modelo de IA de propósito general excepcionalmente no presenta riesgos sistémicos y que, por tanto, no debe clasificarse como modelo de IA de propósito general con riesgos sistémicos. Esa información es valiosa para que la Oficina de IA pueda anticiparse a la comercialización de modelos de IA de propósito general con riesgos sistémicos y los proveedores puedan empezar a colaborar con la Oficina de IA desde el principio. Esta información es especialmente importante por lo que respecta a los modelos de IA de propósito general que está previsto comercializar como código abierto, dado que, tras
de código abierto, puede resultar más difícil aplicar las medidas necesarias para garantizar el cumplimiento de las obligaciones establecidas en el presente Reglamento.

(113) Si la Comisión tiene conocimiento de que un modelo de IA de propósito general cumple los requisitos para ser clasificado como modelo de IA de propósito general con riesgo sistémico, lo que anteriormente no se sabía o no había sido notificado a la Comisión por el proveedor correspondiente, la Comisión debe estar facultada para designarlo como tal. Un sistema de alertas cualificadas debe garantizar que el panel científico ponga en conocimiento de la Oficina de IA los modelos de IA de propósito general que posiblemente deban clasificarse como modelos de IA de propósito general con riesgo sistémico, además de las actividades de supervisión de la Oficina de IA.

(114) Los proveedores de modelos de IA de propósito general que presenten riesgos sistémicos deben estar sujetos, además de a las obligaciones previstas para los proveedores de modelos de IA de propósito general, a obligaciones destinadas a identificar y mitigar dichos riesgos y a garantizar un nivel adecuado de protección de la ciberseguridad, independientemente de si se proporciona como modelo independiente o integrado en un sistema o producto de IA. Para alcanzar estos objetivos, el presente Reglamento debe exigir a los proveedores que realicen las evaluaciones necesarias de los modelos, en particular antes de su primera comercialización, incluyendo la realización y documentación de pruebas adversariales de los modelos, también, según proceda, mediante pruebas internas o externas independientes. Además, los proveedores de modelos de IA de propósito general con riesgos sistémicos deben evaluar y mitigar continuamente los riesgos sistémicos, por ejemplo estableciendo políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, aplicando un seguimiento posterior a la comercialización, adoptando medidas adecuadas a lo largo de todo el ciclo de vida del modelo y cooperando con los agentes pertinentes a lo largo de la cadena de valor de la IA.

(115) ***Los proveedores de modelos de IA de propósito general con riesgos sistémicos deben evaluar y mitigar los posibles riesgos sistémicos. Si, a pesar de los esfuerzos por identificar y prevenir los riesgos relacionados con un modelo de IA de propósito general que pueda presentar riesgos sistémicos, el desarrollo o el uso del modelo provoca un incidente grave, el proveedor del modelo de IA de propósito general deberá, sin demora indebida, hacer un seguimiento del incidente y comunicar toda la información pertinente y las posibles medidas correctoras a la Comisión y a las autoridades nacionales competentes. Además, los proveedores deben garantizar un nivel adecuado de protección de la ciberseguridad para el modelo y su infraestructura física, en su caso, a lo largo de todo el ciclo de vida del modelo. La protección de la ciberseguridad relacionada con los riesgos sistémicos asociados al uso malintencionado o a los ataques debe tener debidamente en cuenta las fugas accidentales de modelos, las liberaciones no autorizadas, la elusión de las medidas de seguridad y la defensa contra los ciberataques, el acceso no autorizado o el robo de modelos. Esa protección podría facilitarse asegurando las ponderaciones de los modelos, los algoritmos, los servidores y los conjuntos de datos, por ejemplo mediante medidas de seguridad operativa para la seguridad de la información, políticas específicas de ciberseguridad, soluciones técnicas adecuadas y establecidas, y controles de acceso cibernético y físico, adecuados a las circunstancias pertinentes y a los riesgos existentes.***

(116) La Oficina de IA debería fomentar y facilitar la elaboración, revisión y adaptación de códigos de buenas prácticas, teniendo en cuenta los planteamientos internacionales. Podría invitarse a participar a todos los proveedores de modelos de IA de uso general. Para garantizar que los códigos de buenas prácticas reflejen el estado actual de la técnica y tengan debidamente en cuenta un conjunto diverso de perspectivas, la Oficina de la IA debería colaborar con las autoridades nacionales competentes y, en su caso, podría consultar a las organizaciones de la sociedad civil y a otras partes interesadas y expertos pertinentes, incluida la Comisión Técnica Científica, para la elaboración de dichos códigos. Los códigos de buenas prácticas deben abarcar las obligaciones de los proveedores de modelos de IA de propósito general y de modelos de propósito general que presenten riesgos sistémicos. Además, por lo que se refiere a los riesgos sistémicos, los códigos de buenas prácticas deben contribuir a establecer una taxonomía de riesgos del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes. Los códigos de buenas prácticas también deberían centrarse en medidas específicas de evaluación y mitigación de riesgos.

(117) ***Los códigos de buenas prácticas deben representar una herramienta central para el correcto cumplimiento de las obligaciones previstas en el presente Reglamento para los proveedores de modelos de IA de propósito general. Los proveedores deben poder basarse en los códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Mediante actos de ejecución, la Comisión puede decidir aprobar un código de buenas prácticas y darle una validez general en la Unión o, alternativamente, establecer normas comunes para la aplicación de las obligaciones pertinentes, si, en el momento en que el presente Reglamento sea aplicable, no se puede ultimar un código de buenas prácticas o la Oficina de IA no lo considera adecuado. Una vez publicada una norma armonizada y evaluada como adecuada para cubrir las obligaciones pertinentes por la Oficina de IA, el cumplimiento de una norma armonizada europea debe otorgar a los proveedores la presunción de conformidad. Además, los proveedores de modelos de IA de uso general deben poder demostrar el cumplimiento utilizando medios alternativos adecuados, si no se dispone de códigos de prácticas o normas armonizadas, o si deciden no basarse en ellos.***

(118) El presente Reglamento regula los sistemas y modelos de IA imponiendo determinados requisitos y obligaciones a los agentes del mercado pertinentes que los comercialicen, pongan en servicio o utilicen en la Unión, complementando así las obligaciones para los proveedores de servicios de intermediación que integren dichos sistemas o modelos en sus servicios regulados por el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo[42]. En la medida en que tales sistemas o modelos estén integrados en plataformas en línea muy grandes o motores de búsqueda en línea muy grandes designados, estarán sujetos al marco de gestión de riesgos previsto en el Reglamento (UE) 2022/2065. En consecuencia, debe presumirse que se cumplen las obligaciones correspondientes del presente Reglamento, a menos que surjan y se identifiquen en dichos modelos riesgos sistémicos significativos no cubiertos por el Reglamento (UE) 2022/2065. En este marco, los proveedores de plataformas en línea muy grandes y de motores de búsqueda en línea muy grandes están obligados a evaluar los riesgos sistémicos potenciales derivados del diseño, el funcionamiento y el uso de sus servicios, incluido el modo en que el diseño de los sistemas algorítmicos utilizados en el servicio puede contribuir a tales riesgos, así como los riesgos sistémicos derivados de posibles usos indebidos. Dichos proveedores también están obligados a adoptar las medidas paliativas adecuadas en observancia de los derechos fundamentales.

---

42 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de servicios digitales) (DO L 277 de 27.10.2022, p. 1).

(119) Teniendo en cuenta el rápido ritmo de la innovación y la evolución tecnológica de los servicios digitales en el ámbito de aplicación de diferentes instrumentos del Derecho de la Unión, en particular teniendo en cuenta el uso y la percepción de sus destinatarios, los sistemas de IA sujetos al presente Reglamento pueden prestarse como servicios de intermediación o partes de los mismos en el sentido del Reglamento (UE) 2022/2065, que debe interpretarse de manera tecnológicamente neutra. Por ejemplo, los sistemas de IA pueden utilizarse para proporcionar motores de búsqueda en línea, en particular, en la medida en que un sistema de IA como un chatbot en línea realiza búsquedas de, en principio, todos los sitios web, a continuación incorpora los resultados a sus conocimientos existentes y utiliza los conocimientos actualizados para generar un único resultado que combina diferentes fuentes de información.

(120) Además, las obligaciones impuestas a los proveedores e implantadores de determinados sistemas de IA en el presente Reglamento para permitir la detección y divulgación de que los resultados de dichos sistemas se han generado o manipulado artificialmente son especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular a las obligaciones de los proveedores de plataformas en línea muy grandes o de motores de búsqueda en línea muy grandes de identificar y mitigar los riesgos sistémicos que puedan derivarse de la difusión de contenidos generados o manipulados artificialmente, en particular el riesgo de los efectos negativos reales o previsibles en los procesos democráticos, el discurso cívico y los procesos electorales, incluso a través de la desinformación.

(121) La normalización debe desempeñar un papel clave para ofrecer soluciones técnicas a los proveedores que garanticen el cumplimiento del presente Reglamento***, en consonancia con el estado de la técnica, a fin de promover la innovación, así como la competitividad y el crecimiento en el mercado único***. El cumplimiento de las normas armonizadas definidas en el artículo 2, punto 1, letra c), del Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del **Consejo**[43]***, que normalmente se espera que reflejen el estado de la técnica,*** debe ser un medio para que los proveedores demuestren la conformidad con los requisitos del presente Reglamento. ***Por consiguiente, debe fomentarse una representación equilibrada de los intereses en la que participen todas las partes interesadas pertinentes en la elaboración de las normas, en particular las PYME, las organizaciones de consumidores y las partes interesadas medioambientales y sociales, de conformidad con los artículos 5 y 6 del Reglamento (UE) nº 1025/2012. Para facilitar el cumplimiento, la Comisión debe emitir las solicitudes de normalización sin demoras indebidas. Al preparar la solicitud de normalización, la Comisión debe consultar al foro consultivo y a la Junta para recabar los conocimientos técnicos pertinentes. No*** obstante, a ***falta de referencias pertinentes a normas armonizadas,*** la Comisión ***debe poder establecer, mediante actos de ejecución y previa consulta al foro consultivo, especificaciones comunes para determinados requisitos del presente Reglamento.***

---

43 Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea y por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y se derogan la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

La especificación común ***debe ser una solución de emergencia excepcional para facilitar la obligación del proveedor de cumplir los requisitos del presente Reglamento, cuando la solicitud de normalización no haya sido aceptada por ninguna de las organizaciones europeas de normalización, o cuando las normas armonizadas pertinentes no aborden suficientemente las preocupaciones en materia de derechos fundamentales, o cuando las normas*** armonizadas ***no se ajusten a la solicitud, o cuando se produzcan retrasos en la adopción de una norma armonizada adecuada***. ***Cuando dicho retraso en la adopción de una norma armonizada se deba a la complejidad técnica de dicha norma, la Comisión deberá tenerlo en cuenta antes de contemplar el establecimiento de especificaciones comunes. A la hora de desarrollar especificaciones comunes, se anima a la Comisión a cooperar con socios internacionales y organismos internacionales de normalización.***

(122) Conviene que, sin perjuicio del uso de normas armonizadas y especificaciones comunes, se presuma que los proveedores de sistemas de IA de alto riesgo que hayan sido formados y probados con datos que reflejen el entorno geográfico, conductual, contextual o funcional específico en el que se pretende utilizar el sistema de IA cumplen la medida pertinente prevista en el requisito sobre gobernanza de datos establecido en el presente Reglamento. Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, de conformidad con el artículo 54, apartado 3, del Reglamento (UE) 2019/881 del Parlamento Europeo y del *Consejo44*, ***debe presumirse que los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya expedido una declaración de conformidad en el marco de un régimen de ciberseguridad con arreglo a dicho Reglamento y cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea cumplen el requisito de ciberseguridad del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad o partes de los mismos cubran el requisito de ciberseguridad del presente Reglamento Esto se mantiene sin perjuicio del carácter voluntario de dicho régimen de ciberseguridad.***

(123) Para garantizar un alto nivel de fiabilidad de los sistemas de IA de alto riesgo, dichos sistemas deben someterse a una evaluación de conformidad antes de su comercialización o puesta en servicio.

---

44 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a la ENISA (Agencia de Ciberseguridad de la Unión Europea) y a la certificación de la ciberseguridad de las tecnologías de la información y las comunicaciones y por el que se deroga el Reglamento (UE) n.º 526/2013 (Ley de Ciberseguridad) (DO L 151 de 7.6.2019, p. 15).

(124) Conviene que, para minimizar la carga de los operadores y evitar cualquier posible duplicación, en el caso de los sistemas de IA de alto riesgo relacionados con productos que estén cubiertos por la legislación de armonización de la Unión vigente basada en el nuevo marco legislativo, la conformidad de dichos sistemas de IA con los requisitos del presente Reglamento se evalúe como parte de la evaluación de la conformidad ya prevista en dicha legislación. Así pues, la aplicabilidad de los requisitos del presente Reglamento no debe afectar a la lógica específica, la metodología o la estructura general de la evaluación de la conformidad con arreglo a la legislación de armonización de la Unión pertinente. ▌

(125) Dada la ***complejidad de los sistemas de IA de alto riesgo y los riesgos que llevan asociados, es importante desarrollar un sistema adecuado de procedimiento de evaluación de la conformidad para los sistemas de IA de alto riesgo en el que participen organismos notificados, la denominada evaluación de la conformidad por terceros. No obstante, habida cuenta de la*** experiencia actual de los certificadores profesionales previos a la comercialización en el ámbito de la seguridad de los productos y de la diferente naturaleza de los riesgos implicados, conviene limitar, al menos en una fase inicial de aplicación del presente Reglamento, el ámbito de aplicación de la evaluación de la conformidad por terceros para los sistemas de IA de alto riesgo distintos de los relacionados con los productos. Por lo tanto, la evaluación de la conformidad de dichos sistemas debe realizarla, como norma general, el proveedor bajo su propia responsabilidad, con la única excepción de los sistemas de IA destinados a ser utilizados para la ***biometría***.

(126) ***Con el fin de llevar a cabo evaluaciones de*** la conformidad por terceros ***cuando así se requiera***, los organismos notificados deben ser ***notificados*** con arreglo al presente Reglamento por las autoridades nacionales competentes, siempre que cumplan una serie de requisitos, en particular sobre independencia, competencia, ausencia de conflictos de intereses ***y requisitos de ciberseguridad adecuados***. ***Las autoridades nacionales competentes deben enviar la notificación de dichos organismos a la Comisión y a los demás Estados miembros por medio de la herramienta de notificación electrónica desarrollada y gestionada por la Comisión con arreglo al artículo R23 del anexo I de la Decisión nº 768/2008/CE.***

(127) En consonancia con los compromisos de la Unión en virtud del Acuerdo sobre Obstáculos Técnicos al Comercio de la Organización Mundial del Comercio, es adecuado facilitar el reconocimiento mutuo de los resultados de la evaluación de la conformidad producidos por organismos de evaluación de la conformidad competentes, independientemente del territorio en el que estén establecidos, siempre que dichos organismos de evaluación de la conformidad establecidos con arreglo a la legislación de un tercer país cumplan los requisitos aplicables del presente Reglamento y la Unión haya celebrado un acuerdo en ese sentido. En este contexto, la Comisión debe explorar activamente posibles instrumentos internacionales a tal efecto y, en particular, perseguir la celebración de acuerdos de reconocimiento mutuo con terceros países.

(128) En consonancia con el concepto comúnmente establecido de modificación sustancial de los productos regulados por la legislación de armonización de la Unión, conviene que ▌ siempre que se produzca un cambio que pueda afectar a la conformidad de un sistema de IA ***de alto riesgo*** con el presente Reglamento ***(por ejemplo, cambio del sistema operativo o de la arquitectura del software),*** o cuando cambie la finalidad prevista del sistema***, dicho sistema de IA debe considerarse un nuevo sistema de IA que debe someterse a una nueva evaluación de la conformidad. No obstante, los cambios que se produzcan en el algoritmo y el rendimiento de*** los sistemas de IA que sigan "aprendiendo" después de su introducción en el mercado o puesta en servicio, es decir, ▌ ***adaptando automáticamente*** la forma en que se llevan a cabo las funciones, ***no deben constituir una modificación sustancial, siempre que dichos cambios*** hayan sido predeterminados por el proveedor y evaluados en el momento de la evaluación de la conformidad ▌ .

(129) Los sistemas de IA de alto riesgo deben llevar el marcado CE para indicar su conformidad con el presente Reglamento, de modo que puedan circular libremente en el mercado interior. ***En el caso de los sistemas de IA de alto riesgo integrados en un producto, debe colocarse un marcado CE físico, que puede complementarse con un marcado CE digital. En el caso de los sistemas de IA de alto riesgo suministrados únicamente de forma digital, debe utilizarse un marcado CE digital.*** Los Estados miembros no deben crear obstáculos injustificados a la comercialización o puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(130) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas***, la protección del medio ambiente y el cambio climático*** y para la sociedad en su conjunto. Así pues, conviene que, por razones excepcionales de ***seguridad pública o de*** protección de la vida y la salud de las personas físicas***, de protección del medio ambiente*** y de protección de ***activos industriales e infraestructurales clave, las autoridades de vigilancia del mercado*** puedan autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA que no hayan sido sometidos a una evaluación de la conformidad. ***En situaciones debidamente justificadas con arreglo a lo dispuesto en el presente Reglamento, las autoridades policiales o de protección civil podrán poner en servicio un sistema de IA específico de alto riesgo sin la autorización de la autoridad de vigilancia del mercado, siempre que dicha autorización se solicite durante o después de la utilización sin demora indebida.***

(131) Para facilitar el trabajo de la Comisión y de los Estados miembros en el ámbito de la IA, así como para aumentar la transparencia de cara al público, debe exigirse a los proveedores de sistemas de IA de alto riesgo distintos de los relacionados con productos incluidos en el ámbito de aplicación de la legislación de armonización de la Unión vigente pertinente, ***así como a los proveedores que consideren que el sistema de IA de alto riesgo enumerado en un anexo del presente Reglamento no es de alto riesgo sobre la base de una excepción***, que se registren ***y registren la información sobre su sistema de*** IA en una base de datos de la UE, que creará y gestionará la Comisión. ***Antes de utilizar dicho sistema de IA de alto riesgo, los implantadores de sistemas de IA de alto riesgo que sean autoridades, agencias u organismos públicos deben registrarse en dicha base de datos y seleccionar el sistema que prevén utilizar.***

Los demás implantadores deberían tener derecho a hacerlo voluntariamente. Esta sección de la base de datos debe ser de acceso público y gratuito, y la información debe ser fácilmente navegable, comprensible y legible por máquina. La base de datos también debe ser de fácil uso, por ejemplo, proporcionando funcionalidades de búsqueda, incluso mediante palabras clave, que permitan al público en general encontrar la información pertinente que debe presentarse en el momento del registro de los sistemas de IA de alto riesgo y sobre los sistemas de IA de alto riesgo, establecidos en los anexos del presente Reglamento, a los que corresponden los sistemas de IA de alto riesgo. Cualquier modificación sustancial de los sistemas de IA de alto riesgo también deberá registrarse en la base de datos de la UE. En el caso de los sistemas de IA de alto riesgo en el ámbito de la aplicación de la ley, la migración, el asilo y la gestión del control fronterizo, las obligaciones de registro deberán cumplirse en una sección segura no pública de la base de datos. El acceso a la sección no pública segura debe limitarse estrictamente a la Comisión y a las autoridades de vigilancia del mercado en lo que respecta a su sección nacional de la base de datos. Los sistemas de IA de alto riesgo en el ámbito de las infraestructuras críticas sólo deben registrarse a nivel nacional. La Comisión debe ser el controlador de la base de datos de ***la UE***, de conformidad con el Reglamento (UE) 2018/1725. Para garantizar la plena funcionalidad de la base de datos, cuando se despliegue, el procedimiento para establecer la base de datos debe incluir la elaboración de especificaciones funcionales por parte de la Comisión y un informe de auditoría independiente. ***La Comisión debe tener en cuenta los riesgos relacionados con la ciberseguridad y los peligros al desempeñar sus funciones como responsable del tratamiento de datos en la base de datos de la UE.***

Con el fin de maximizar la disponibilidad y el uso de la base de datos por parte del público, la base de datos, incluida la información disponible a través de ella, debe cumplir los requisitos establecidos en la Directiva (UE) 2019/882.

(132) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden plantear riesgos específicos de suplantación de identidad o engaño, con independencia de que se califiquen o no de alto riesgo. En determinadas circunstancias, el uso de estos sistemas debería, por tanto, estar sujeto a obligaciones específicas de transparencia sin perjuicio de los requisitos y obligaciones para los sistemas de IA de alto riesgo ***y sujeto a excepciones específicas para tener en cuenta la necesidad especial de las fuerzas y cuerpos de seguridad***. En particular, debe notificarse a las personas físicas que están interactuando con un sistema de IA, a menos que ello resulte obvio desde el ***punto de vista de una persona física razonablemente bien informada, observadora y perspicaz teniendo en cuenta las*** circunstancias y el contexto de uso. ***Al aplicar dicha obligación, deberán tenerse en cuenta las características de las personas pertenecientes a grupos de personas vulnerables debido a su edad o discapacidad, en la medida en que el sistema de IA esté destinado a interactuar también con dichos grupos. Además, las personas físicas deben ser notificadas cuando estén expuestas a sistemas que, mediante el tratamiento de sus datos biométricos, puedan identificar o inferir las emociones o intenciones de dichas*** personas ***o asignarlas a categorías específicas. Dichas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos personales, el origen étnico, las preferencias personales y los intereses. Dicha información y notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad***.

(133) ***Diversos sistemas de IA pueden generar grandes cantidades de contenidos sintéticos que resultan cada vez más difíciles de distinguir para los humanos de los contenidos auténticos y generados por ellos. La amplia disponibilidad y las crecientes capacidades de esos sistemas tienen un impacto significativo en la integridad y la confianza en el ecosistema de la información, planteando nuevos riesgos de desinformación y manipulación a escala, fraude, suplantación de identidad y engaño al consumidor. A la luz de esas repercusiones, del rápido ritmo tecnológico y de la necesidad de nuevos métodos y técnicas para rastrear el origen de la información, conviene exigir a los proveedores de esos sistemas que incorporen soluciones técnicas que permitan el marcado en un formato legible por máquina y la detección de que el resultado ha sido generado o manipulado por un sistema de IA y no por un ser humano. Dichas técnicas y métodos deben ser suficientemente fiables, interoperables, eficaces y sólidos en la medida en que sea técnicamente viable, teniendo en cuenta las técnicas disponibles o una combinación de dichas técnicas, como marcas de agua, identificaciones de metadatos, métodos criptográficos para demostrar la procedencia y autenticidad de los contenidos, métodos de registro, huellas dactilares u otras técnicas, según proceda. Al aplicar esta obligación, los proveedores también deben tener en cuenta las especificidades y las limitaciones de los diferentes tipos de contenidos y los avances tecnológicos y de mercado pertinentes en este ámbito, tal como se reflejan en el estado de la técnica generalmente reconocido. Dichas técnicas y métodos pueden aplicarse a nivel del sistema o a nivel del modelo, incluidos los modelos de IA de propósito general que generan contenidos, facilitando así el cumplimiento de esta obligación por parte del proveedor posterior del sistema de IA. Para mantener la proporcionalidad, conviene prever que esta obligación de marcado no cubra los sistemas de IA que desempeñen principalmente una función de asistencia para la edición estándar o los sistemas de IA que no alteren sustancialmente los datos de entrada proporcionados por el usuario o la semántica de los mismos.***

(134) Además de las soluciones técnicas empleadas por los proveedores del sistema, quienes utilicen un sistema de IA para generar o manipular contenidos de imagen, audio o vídeo que se parezcan sensiblemente a personas, lugares o acontecimientos existentes y que a una persona le parezcan falsamente auténticos (deep fakes), El cumplimiento de esta obligación de transparencia no debe interpretarse en el sentido de que el uso del sistema o de sus resultados impida el derecho a la libertad de expresión y el derecho a la libertad de las artes y las ciencias garantizados en la Carta, en particular cuando el contenido forme parte de una obra o programa evidentemente creativo, satírico, artístico o de ficción, sin perjuicio de las salvaguardias adecuadas de los derechos y libertades de terceros. En estos casos, la obligación de transparencia para las falsificaciones profundas establecida en el presente Reglamento se limita a la divulgación de la existencia de dichos contenidos generados o manipulados de una manera adecuada que no obstaculice la exhibición o disfrute de la obra, incluida su explotación y uso normales, manteniendo al mismo tiempo la utilidad y calidad de la obra. Además, también procede prever una obligación de divulgación similar en relación con el texto generado o manipulado mediante IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado mediante IA haya sido sometido a un proceso de revisión humana o control editorial y una persona física o jurídica ostente la responsabilidad editorial de la publicación del contenido.

(135) ***Para garantizar una aplicación coherente, conviene facultar a la Comisión para que adopte actos de ejecución sobre la aplicación de las disposiciones relativas al etiquetado y la detección de contenidos generados o manipulados artificialmente. Sin perjuicio del carácter obligatorio y de la plena aplicabilidad de las obligaciones de transparencia, la Comisión también podrá fomentar y facilitar 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 artificialmente, incluido el apoyo a disposiciones prácticas para hacer accesibles, según proceda, los mecanismos de detección y facilitar la cooperación con otros agentes a lo largo de la cadena de valor, difundir contenidos o comprobar su autenticidad y procedencia para permitir al público distinguir efectivamente los contenidos generados por IA.***

(136) Las obligaciones impuestas a los proveedores e implantadores de determinados sistemas de IA en el presente Reglamento para permitir la detección y divulgación de que los resultados de dichos sistemas se han generado o manipulado artificialmente son especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular en lo que respecta a las obligaciones de los proveedores de plataformas en línea muy grandes o de motores de búsqueda en línea muy grandes de identificar y mitigar los riesgos sistémicos que puedan derivarse de la difusión de contenidos que hayan sido generados o manipulados artificialmente, en particular el riesgo de los efectos negativos reales o previsibles en los procesos democráticos, el discurso cívico y los procesos electorales, incluso a través de la desinformación. El requisito de etiquetar los contenidos generados por sistemas de IA con arreglo al presente Reglamento se entiende sin perjuicio de la obligación establecida en el artículo 16, apartado 6, del Reglamento (UE) 2022/2065 de que los proveedores de servicios de alojamiento tramiten las notificaciones sobre contenidos ilícitos recibidas de conformidad con el artículo 16, apartado 1, de dicho Reglamento, y no debe influir en la evaluación y la decisión sobre la ilicitud de los contenidos específicos. Dicha evaluación debe realizarse únicamente con referencia a las normas que rigen la legalidad del contenido.

(137) El cumplimiento de las obligaciones de transparencia de los sistemas de inteligencia artificial contemplados en el presente Reglamento no debe interpretarse como una indicación de que el uso del sistema o de sus resultados es lícito en virtud del presente Reglamento o de otros actos legislativos de la Unión o de los Estados miembros, y debe entenderse sin perjuicio de otras obligaciones de transparencia para los implantadores de sistemas de inteligencia artificial establecidas en el Derecho de la Unión o nacional.

(138) La IA es una familia de tecnologías en rápido desarrollo que requiere una supervisión reglamentaria y un espacio seguro ***y controlado*** para la experimentación, garantizando al mismo tiempo una innovación responsable y la integración de salvaguardias adecuadas y medidas de mitigación de riesgos. Para garantizar un marco jurídico que ***promueva la innovación,*** esté preparado para el futuro y sea resistente a las perturbaciones, los Estados miembros ***deben velar por que sus autoridades nacionales competentes establezcan al menos un espacio*** aislado de regulación de la IA ***a nivel nacional*** para facilitar el desarrollo y la experimentación de sistemas innovadores de IA bajo una estricta supervisión reglamentaria antes de que estos sistemas se comercialicen o se pongan en servicio de otro modo. Los ***Estados miembros también podrían cumplir esta obligación participando en los compartimentos estancos reguladores ya existentes o estableciendo conjuntamente un compartimento estanco con una o más autoridades competentes de los Estados miembros, en la medida en que esta participación proporcione un nivel equivalente de cobertura nacional para los Estados miembros participantes. Los compartimentos estancos reguladores pueden establecerse en forma física, digital o híbrida y pueden dar cabida tanto a productos físicos como digitales. Las autoridades encargadas de su creación también deberán garantizar que los compartimentos estancos de regulación dispongan de los recursos adecuados para su funcionamiento, incluidos los recursos financieros y humanos.***

(139) Los objetivos de los espacios aislados de regulación de la IA deben ser fomentar la innovación en materia de IA mediante el establecimiento de un entorno controlado de experimentación y ensayo en la fase de desarrollo y de precomercialización, con vistas a garantizar la conformidad de los sistemas innovadores de IA con el presente Reglamento y demás legislación nacional y de la Unión pertinente***,*** aumentar la seguridad jurídica de los innovadores y la supervisión y comprensión de las oportunidades por parte de las autoridades competentes, los riesgos emergentes y los impactos del uso de la IA, ***facilitar el aprendizaje normativo para las autoridades y las empresas, también con vistas a futuras adaptaciones del marco jurídico, apoyar la cooperación y el intercambio de mejores prácticas con las autoridades que participan en el espacio aislado de regulación de la IA,*** y acelerar el acceso a los mercados, también mediante la eliminación de obstáculos para las PYME***, incluidas*** las empresas de nueva creación. ***Los entornos aislados de regulación deben estar ampliamente disponibles en toda la*** Unión, ***y debe prestarse especial atención a su accesibilidad para las PYME, incluidas las nuevas empresas. La participación en el espacio aislado de regulación*** de ***la IA debe centrarse en las cuestiones que plantean inseguridad jurídica a los proveedores y posibles proveedores para innovar, experimentar con la IA en la Unión y contribuir al aprendizaje normativo basado en pruebas. Por lo tanto,*** la supervisión de los ***sistemas de IA en el espacio aislado regulador de la IA*** debe ***abarcar su desarrollo, formación, ensayo y validación antes de que los sistemas se comercialicen o se pongan en servicio, así como la noción y ocurrencia de modificaciones sustanciales que puedan requerir un nuevo procedimiento de evaluación de la conformidad. Cualquier riesgo significativo detectado durante el desarrollo y las pruebas de dichos sistemas de*** IA ***debe dar lugar a una mitigación adecuada y, en su defecto,*** a la ***suspensión del proceso de desarrollo y prueba.***

Cuando proceda, las autoridades nacionales competentes que establezcan los entornos aislados reguladores de la IA ***deben cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales, y podrían permitir la participación de otros agentes del ecosistema de la IA, como las organizaciones nacionales o europeas de normalización, los organismos notificados, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación, los Centros Europeos de Innovación Digital y las organizaciones pertinentes de las partes interesadas y de la sociedad civil. Para garantizar una aplicación uniforme en toda la Unión y economías de escala,*** conviene ***establecer normas comunes para la aplicación de los entornos aislados reguladores y un marco de cooperación entre las*** autoridades ***pertinentes que participan en la supervisión de los entornos aislados. Los compartimentos estancos reguladores de la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otras disposiciones legales que permitan el establecimiento de otros compartimentos estancos destinados a garantizar el cumplimiento del Derecho de la Unión distinto del presente Reglamento. Cuando proceda, las autoridades competentes pertinentes encargadas de esos otros entornos aislados de regulación deben considerar las ventajas de utilizarlos también para garantizar la conformidad de los sistemas de IA con el presente Reglamento. Previo acuerdo entre las autoridades nacionales*** competentes ***y los participantes en el espacio aislado de regulación de la IA, también podrán realizarse y supervisarse pruebas en condiciones reales en el marco del espacio aislado de regulación de la IA***.

(140) El presente Reglamento debe proporcionar la base jurídica para que los proveedores y posibles proveedores del espacio aislado de regulación de la IA utilicen los datos personales recogidos con otros fines para desarrollar determinados sistemas de IA en aras del interés público dentro del espacio aislado de regulación de la IA, únicamente en condiciones especificadas, de conformidad con el artículo 6, apartado 4, y el artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679, y los artículos 5, 6 y 10 del Reglamento (UE) 2018/1725, y sin perjuicio del artículo 4, apartado 2, y del artículo 10 de la Directiva (UE) 2016/680. Todas las demás obligaciones de los responsables del tratamiento y los derechos de los interesados en virtud de los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y de la Directiva (UE) 2016/680 siguen siendo aplicables. En particular, el presente Reglamento no debe proporcionar una base jurídica en el sentido del artículo 22, apartado 2, letra b), del Reglamento (UE) 2016/679 y del artículo 24, apartado 2, letra b), del Reglamento (UE) 2018/1725. Los proveedores y posibles proveedores del espacio aislado deben garantizar las salvaguardias adecuadas y cooperar con las autoridades competentes, en particular siguiendo sus orientaciones y actuando con celeridad y de buena fe para mitigar adecuadamente los riesgos significativos identificados para la seguridad, la salud y los derechos fundamentales que puedan surgir durante el desarrollo, las pruebas y la experimentación en el espacio aislado.

(141) Con el fin de acelerar el proceso de desarrollo y la comercialización de los sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, es importante que los proveedores o posibles proveedores de tales sistemas también puedan beneficiarse de un régimen específico para probar dichos sistemas en condiciones del mundo real, sin participar en un espacio aislado de regulación de la IA. No obstante, en tales casos y teniendo en cuenta las posibles consecuencias de tales pruebas para las personas, debe velarse por que el presente Reglamento introduzca garantías y condiciones adecuadas y suficientes para los proveedores o posibles proveedores. Dichas garantías deben incluir, entre otras, la solicitud del consentimiento informado de las personas físicas para participar en las pruebas en condiciones del mundo real, con la excepción de las fuerzas y cuerpos de seguridad, en las que la solicitud del consentimiento informado impediría probar el sistema de IA. El consentimiento de los sujetos para participar en dichas pruebas con arreglo al presente Reglamento es distinto y se entiende sin perjuicio del consentimiento de los interesados para el tratamiento de sus datos personales con arreglo a la legislación pertinente en materia de protección de datos.

También es importante minimizar los riesgos y permitir la supervisión por parte de las autoridades competentes y, por lo tanto, exigir a los posibles proveedores que presenten un plan de pruebas en condiciones reales a la autoridad competente de vigilancia del mercado, que registren las pruebas en secciones específicas de la base de datos de la UE con algunas excepciones limitadas, que establezcan limitaciones sobre el período durante el cual pueden realizarse las pruebas y que exijan salvaguardias adicionales para las personas vulnerables, incluidos los grupos de personas vulnerables, así como un acuerdo por escrito que defina las funciones y responsabilidades de los posibles proveedores e implantadores y la supervisión efectiva por parte del personal competente que participe en las pruebas en condiciones reales. Además, conviene prever salvaguardias adicionales para garantizar que las predicciones, recomendaciones o decisiones del sistema de IA puedan ser efectivamente anuladas e ignoradas y que los datos personales estén protegidos y se supriman cuando los sujetos hayan retirado su consentimiento para participar en las pruebas, sin perjuicio de sus derechos como interesados en virtud de la legislación de la Unión sobre protección de datos. Por lo que se refiere a la transferencia de datos, también conviene prever que los datos recogidos y tratados a efectos de pruebas en condiciones reales solo se transfieran a terceros países cuando se apliquen las garantías adecuadas y aplicables en virtud del Derecho de la Unión, en particular de conformidad con las bases para la transferencia de datos personales en virtud del Derecho de la Unión sobre protección de datos, mientras que para los datos no personales se establezcan las garantías adecuadas de conformidad con el Derecho de la Unión, como los Reglamentos (UE) *2022/86845* ***y*** (UE) *2023/285446* del Parlamento Europeo y del Consejo***.***

---

45 Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de gobernanza de datos) (DO L 152 de 3.6.2022, p. 1).

46 Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, relativo a normas armonizadas sobre el acceso y el uso leales de los datos y por el

que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Ley de datos) (DO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) Para garantizar que la IA conduzca a resultados social y ambientalmente beneficiosos, se anima a los Estados miembros a que apoyen y promuevan la investigación y el desarrollo de soluciones de IA en apoyo de resultados social y ambientalmente beneficiosos, como soluciones basadas en la IA para aumentar la accesibilidad de las personas con discapacidad, abordar las desigualdades socioeconómicas o cumplir objetivos medioambientales, asignando recursos suficientes, incluida financiación pública y de la Unión, y, cuando proceda y siempre que se cumplan los criterios de admisibilidad y selección, considerando en particular los proyectos que persigan tales objetivos. Dichos proyectos deberían basarse en el principio de cooperación interdisciplinar entre desarrolladores de IA, expertos en desigualdad y no discriminación, accesibilidad, derechos de los consumidores, medioambientales y digitales, así como académicos.

(143) Para promover y proteger la innovación, es importante que se tengan especialmente en cuenta los intereses de ***las PYME, incluidas las de nueva creación, que son proveedoras o implantadoras*** de sistemas de IA. Con este objetivo, los Estados miembros deberán desarrollar iniciativas dirigidas a dichos operadores, que incluyan ***la*** sensibilización y la comunicación de información. ***Los Estados miembros proporcionarán a las PYME, incluidas las de nueva creación, que tengan un domicilio social o una sucursal en la Unión, acceso prioritario a los entornos aislados reguladores de la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección y sin impedir que otros proveedores y posibles proveedores accedan a los entornos aislados siempre que cumplan las mismas condiciones y criterios. Los Estados miembros utilizarán los canales existentes y, cuando proceda, establecerán nuevos canales específicos para la comunicación con las PYME, las empresas de nueva creación, los implantadores, otros innovadores y, en su caso, las autoridades públicas locales, con el fin de apoyar a las PYME a lo largo de su trayectoria de desarrollo, proporcionándoles orientación y respondiendo a sus preguntas sobre la aplicación del presente Reglamento. Cuando proceda, estos canales trabajarán conjuntamente para crear sinergias y garantizar la homogeneidad de sus orientaciones a las PYME, incluidas las empresas emergentes, y a los implantadores. Además, los Estados miembros deben facilitar la participación de las PYME y otras partes interesadas pertinentes en los procesos de desarrollo de la normalización. Por*** otra parte, ***deben tenerse en cuenta los*** intereses y necesidades específicos de las PYME, incluidas las de nueva creación***,*** cuando los organismos notificados fijen las tasas de evaluación de la conformidad. ***La Comisión debe evaluar periódicamente los costes de certificación y conformidad para las PYME, incluidas las de nueva creación, mediante consultas transparentes a los proveedores, y debe colaborar con los Estados miembros para reducir dichos costes.***

Por ejemplo, los costes de traducción relacionados con la documentación obligatoria y la comunicación con las autoridades pueden constituir un coste significativo para los proveedores y otros operadores, en particular los de menor escala. Es posible que los Estados miembros deban garantizar que una de las lenguas determinadas y aceptadas por ellos para la documentación pertinente de los proveedores y para la comunicación con los operadores sea una que comprenda ampliamente el mayor número posible de ***implantadores trans***fronterizos***. A fin de atender las necesidades específicas de las PYME, incluidas las de nueva creación, la Comisión debe facilitar plantillas normalizadas para los ámbitos cubiertos por el presente Reglamento a petición del Consejo. Además, la Comisión debe complementar los esfuerzos de los Estados miembros proporcionando una plataforma de información única con información fácil de usar en relación con el presente Reglamento para todos los proveedores y desplegadores, organizando campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento, y evaluando y promoviendo la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA. Las medianas empresas que hayan sido recientemente pequeñas empresas en el sentido del anexo de la Recomendación*** *2003/361/CE* ***de la Comisión47 deben tener acceso a esas medidas de apoyo, ya que esas nuevas medianas empresas pueden carecer a veces de los recursos jurídicos y la formación necesarios para garantizar la comprensión y el cumplimiento adecuados del presente Reglamento***.

47 Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

(144) Con el fin de promover y proteger la innovación, la plataforma de IA a petición, todos los programas y proyectos de financiación pertinentes de la Unión, como el Programa Europa Digital, Horizonte Europa, ejecutados por la Comisión y los Estados miembros a nivel de la Unión o nacional deben contribuir, según proceda, a la consecución de los objetivos del presente Reglamento.

(145) ***En particular, con el*** fin de minimizar los riesgos para la aplicación derivados de la falta de conocimientos y experiencia en el mercado, así como de facilitar el cumplimiento por parte de los proveedores***, en particular las PYME, incluidas las empresas de nueva creación,*** y los organismos notificados de las obligaciones que les impone el presente Reglamento, la plataforma de IA a petición, los Centros Europeos de Innovación Digital y las instalaciones de ensayo y experimentación establecidas por la Comisión y los Estados miembros a nivel de la Unión o nacional deben contribuir a la aplicación del presente Reglamento. Dentro de sus respectivas misiones y ámbitos de competencia, la plataforma de IA a petición, los Centros Europeos de Innovación Digital y las instalaciones de ensayo y experimentación pueden prestar, en particular, apoyo técnico y científico a los proveedores y a los organismos notificados.

(146) Además, habida cuenta del tamaño muy reducido de algunos operadores y con el fin de garantizar la proporcionalidad en lo que respecta a los costes de la innovación, conviene permitir a las microempresas cumplir una de las obligaciones más costosas, a saber, establecer un sistema de gestión de la calidad, de una manera simplificada que reduciría la carga administrativa y los costes para dichas empresas sin afectar al nivel de protección ni a la necesidad de cumplir los requisitos para los sistemas de IA de alto riesgo. La Comisión debería elaborar directrices para especificar los elementos del sistema de gestión de la calidad que deben cumplir de esta manera simplificada las microempresas.

(147) Conviene que la Comisión facilite, en la medida de lo posible, el acceso a las instalaciones de ensayo y experimentación a los organismos, grupos o laboratorios establecidos o acreditados con arreglo a cualquier legislación de armonización de la Unión pertinente y que desempeñen tareas en el contexto de la evaluación de la conformidad de los productos o dispositivos cubiertos por dicha legislación de armonización de la Unión. Este es, en particular, el caso de los paneles de expertos, los laboratorios de expertos y los laboratorios de referencia en el ámbito de los productos sanitarios con arreglo a los Reglamentos (UE) 2017/745 y (UE) 2017/746.

(148) El presente Reglamento debe establecer un marco de gobernanza que permita tanto coordinar y apoyar la aplicación del presente Reglamento a nivel nacional, como crear capacidades a nivel de la Unión e integrar a las partes interesadas en el ámbito de la IA. La aplicación y el cumplimiento efectivos del presente Reglamento requieren un marco de gobernanza que permita coordinar y crear competencias centrales a nivel de la Unión. La Oficina de Inteligencia Artificial fue creada por Decisión de la Comisión[48] y su misión consiste en desarrollar los conocimientos y capacidades de la Unión en el ámbito de la inteligencia artificial y contribuir a la aplicación de la legislación de la Unión en este ámbito. Los Estados miembros deben facilitar las tareas de la Oficina de la IA con vistas a apoyar el desarrollo de los conocimientos y capacidades de la Unión a nivel de la Unión y reforzar el funcionamiento del mercado único digital. Además, debe crearse un Consejo compuesto por representantes de los Estados miembros, un panel científico que integre a la comunidad científica y un foro consultivo que contribuya con aportaciones de las partes interesadas a la aplicación del presente Reglamento, a escala de la Unión y nacional. El desarrollo de los conocimientos y capacidades de la Unión también debe incluir el aprovechamiento de los recursos y conocimientos existentes, en particular mediante sinergias con las estructuras creadas en el contexto de la aplicación a nivel de la Unión de otras leyes y sinergias con iniciativas conexas a nivel de la Unión, como la Empresa Común EuroHPC y las instalaciones de ensayo y experimentación de la IA en el marco del Programa Europa Digital.

---

48 Decisión de la Comisión de 24.1.2024 por la que se crea la Oficina Europea de Inteligencia Artificial C(2024) 390.

(149) Para facilitar una aplicación fluida, eficaz y armonizada del presente Reglamento, debe crearse un Consejo. El Consejo debe ***reflejar los diversos intereses del ecosistema de la IA y estar compuesto por representantes de los Estados miembros. La Junta debe*** ser responsable de una serie de tareas consultivas, entre ellas emitir dictámenes, recomendaciones, asesoramiento o ***contribuir a la*** orientación sobre asuntos relacionados con la aplicación del presente Reglamento, incluidas las ***cuestiones de ejecución, las*** especificaciones técnicas o las normas existentes relativas a los requisitos establecidos en el presente Reglamento, y asesorar a ***la Comisión y a los Estados miembros y a sus autoridades nacionales competentes*** sobre cuestiones específicas relacionadas con la IA. Con el ***fin de dar cierta flexibilidad a los Estados miembros en la designación de sus representantes en el Consejo, dichos representantes podrán ser personas pertenecientes a entidades públicas que deberán tener las competencias y facultades pertinentes para facilitar la coordinación a nivel nacional y contribuir a la realización de las tareas del Consejo. El Consejo debe crear dos subgrupos permanentes que sirvan de plataforma para la cooperación y el intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas, respectivamente, con la vigilancia del mercado y los organismos notificados. El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020. De conformidad con el artículo 33 de dicho Reglamento, la Comisión debe apoyar las actividades del subgrupo permanente de vigilancia del mercado realizando evaluaciones o estudios de mercado, en particular con vistas a determinar los aspectos del presente Reglamento que requieran una coordinación específica y urgente entre las autoridades de vigilancia del mercado. El Consejo podrá crear otros subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas. El Consejo también debe cooperar, según proceda, con los organismos, grupos de expertos y redes pertinentes de la Unión activos en el contexto de la legislación pertinente de la Unión, incluidos, en particular, los activos en virtud de la legislación pertinente de la Unión sobre datos, productos digitales y servicios.***

(150) Con vistas a garantizar la participación de las partes interesadas en la ejecución y aplicación del presente Reglamento, debe crearse un foro consultivo que asesore y aporte conocimientos técnicos al Consejo y a la Comisión. Para garantizar una representación variada y equilibrada de las partes interesadas entre intereses comerciales y no comerciales y, dentro de la categoría de intereses comerciales, con respecto a las PYME y otras empresas, el foro consultivo debe incluir, entre otros, a la industria, las nuevas empresas, las PYME, el mundo académico, la sociedad civil, incluidos los interlocutores sociales, así como la Agencia de los Derechos Fundamentales, ENISA, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI).

(151) Para apoyar la aplicación y el cumplimiento del presente Reglamento, en particular las actividades de supervisión de la Oficina de IA por lo que respecta a los modelos de IA de uso general, debe crearse un panel científico de expertos independientes. Los expertos independientes que constituyan el panel científico deben ser seleccionados sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA y deben desempeñar sus tareas con imparcialidad y objetividad y garantizar la confidencialidad de la información y los datos obtenidos en el desempeño de sus tareas y actividades. Para permitir el refuerzo de las capacidades nacionales necesarias para la aplicación efectiva del presente Reglamento, los Estados miembros deben poder solicitar el apoyo del grupo de expertos que constituye el panel científico para sus actividades de aplicación.

(152) Para apoyar una aplicación adecuada en lo que respecta a los sistemas de IA y reforzar las capacidades de los Estados miembros, deben crearse estructuras de apoyo a las pruebas de IA de la Unión y ponerlas a disposición de los Estados miembros.

(153) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución del presente Reglamento. A este respecto, cada Estado miembro debe designar al menos ***una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a efectos*** de la supervisión de la aplicación y ejecución del presente Reglamento. Los Estados ***miembros pueden decidir designar cualquier tipo de entidad pública para desempeñar las funciones de las autoridades nacionales competentes en el sentido del presente Reglamento, de acuerdo con sus características y necesidades organizativas nacionales específicas. A*** fin de aumentar la eficiencia organizativa por parte de los Estados miembros y de establecer ***un punto de contacto único*** con el público y otros interlocutores a nivel de los Estados miembros y de la Unión, ▌ cada Estado miembro ***debe designar una autoridad de vigilancia del mercado que actúe como punto de contacto único***.

(154) Las autoridades nacionales competentes deben ejercer sus competencias con independencia, imparcialidad y sin prejuicios, a fin de salvaguardar los principios de objetividad de sus actividades y tareas y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de estas autoridades deben abstenerse de toda acción incompatible con sus funciones y deben estar sujetos a las normas de confidencialidad previstas en el presente Reglamento.

(155) Con el fin de garantizar que los proveedores de sistemas de IA de alto riesgo puedan tener en cuenta la experiencia sobre el uso de sistemas de IA de alto riesgo para mejorar sus sistemas y el proceso de diseño y desarrollo o puedan adoptar cualquier posible medida correctiva de manera oportuna, todos los proveedores deben contar con un sistema de seguimiento posterior a la comercialización. ***Cuando proceda, el seguimiento posterior a la comercialización deberá incluir un análisis de la interacción con otros sistemas de IA, incluidos otros dispositivos y programas informáticos. El seguimiento posterior a la comercialización no debe abarcar los datos operativos sensibles de los implantadores que sean autoridades policiales.*** Este sistema también es clave para garantizar que los posibles riesgos que surjan de los sistemas de IA que siguen "aprendiendo" después de su comercialización o puesta en servicio puedan abordarse de manera más eficiente y oportuna. En este contexto, también debe exigirse a los proveedores que dispongan de un sistema para notificar a las autoridades pertinentes cualquier incidente grave ***derivado del uso de sus sistemas de IA, es decir, incidentes o fallos de funcionamiento que provoquen la muerte o daños graves para la salud, perturbaciones graves e irreversibles de la gestión y el funcionamiento de infraestructuras críticas, infracciones de las obligaciones derivadas del*** Derecho de la Unión ***destinadas a proteger*** los derechos fundamentales ***o daños graves a la propiedad o al medio ambiente***.

(156) A fin de garantizar una aplicación adecuada y efectiva de los requisitos y obligaciones establecidos en el presente Reglamento, que es legislación de armonización de la Unión, debe aplicarse en su totalidad el sistema de vigilancia del mercado y conformidad de los productos establecido en el Reglamento (UE) 2019/1020. Las ***autoridades de vigilancia del mercado designadas de conformidad con el presente Reglamento deben tener todas las competencias de ejecución establecidas en el presente Reglamento y en el Reglamento (UE) 2019/1020, y deben ejercer*** sus ***competencias y desempeñar sus funciones de manera independiente, imparcial y no sesgada. Aunque la mayoría de los sistemas de IA no están sujetos a requisitos y obligaciones específicos en virtud del presente Reglamento,*** las autoridades de ***vigilancia del mercado pueden adoptar medidas en relación con todos los sistemas de IA cuando presenten un riesgo de conformidad con el presente Reglamento. Debido a la naturaleza específica de las instituciones, agencias y*** organismos de ***la Unión que entran en el ámbito de aplicación del presente Reglamento, procede designar al Supervisor Europeo de Protección de Datos como autoridad de vigilancia del mercado competente para ellos. Ello debe entenderse sin perjuicio de la designación de autoridades nacionales competentes por parte de los Estados miembros. Las actividades de vigilancia del mercado no*** deben ***afectar a la capacidad de las entidades supervisadas para llevar a cabo sus tareas de forma independiente, cuando dicha independencia sea exigida por el Derecho de la Unión***.

(157) ***El presente Reglamento se entiende sin perjuicio de las competencias, funciones, facultades e independencia de las autoridades u organismos públicos nacionales pertinentes que supervisan la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de promoción de la igualdad y las autoridades de protección de datos. Cuando sea necesario para su mandato, dichas autoridades u organismos públicos nacionales también deben tener acceso a cualquier documentación creada en virtud del presente Reglamento. Debe establecerse un procedimiento de salvaguardia específico para garantizar una aplicación adecuada y oportuna contra los sistemas de IA que presenten un riesgo para la salud, la seguridad y los derechos fundamentales. El procedimiento para los sistemas de IA que presenten un riesgo debe aplicarse a los sistemas de IA de alto riesgo que presenten un riesgo, a los sistemas prohibidos que se hayan comercializado, puesto en servicio o utilizado infringiendo las prácticas prohibidas establecidas en el presente Reglamento y a los sistemas de IA que se hayan puesto a disposición infringiendo los requisitos de transparencia establecidos en el presente Reglamento y presenten un riesgo.***

(158) El Derecho de la Unión en materia de servicios financieros incluye normas y requisitos internos de gobernanza y gestión de riesgos que son aplicables a las entidades financieras reguladas en el marco de la prestación de dichos servicios, incluso cuando hacen uso de sistemas de IA. A fin de garantizar la aplicación y el cumplimiento coherentes de las obligaciones derivadas del presente Reglamento y de las normas y requisitos pertinentes de los actos jurídicos de la Unión en materia de servicios financieros, las ***autoridades competentes*** para la supervisión y el cumplimiento de dichos actos jurídicos, en particular ***las autoridades competentes definidas en el Reglamento (UE) nº 575/2013 del Parlamento Europeo y del*** *Consejo*[49] ***y las Directivas*** *2008/48/CE*[50]***,*** *2009/138/CE*[51]***,*** *2013/36/UE*[52] *2014/17/UE*[53] ***y (UE)*** 2016/9754del ***Parlamento*** Europeo ***y del Consejo***, deben ser designadas***, en el marco de sus respectivas competencias,*** como autoridades competentes a efectos de la supervisión de la aplicación del presente Reglamento, incluidas las actividades de vigilancia del mercado, por lo que respecta a los sistemas de IA proporcionados o utilizados por las entidades financieras reguladas y supervisadas, ***a menos que los Estados miembros decidan designar a otra autoridad para desempeñar estas funciones de vigilancia del mercado.***

---

49 Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).

50 Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo (DO L 133 de 22.5.2008, p. 66).

51 Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1).

52 Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

53 Directiva 2014/17/UE del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, sobre los contratos de crédito al consumo para bienes inmuebles de uso residencial y por la que se modifican las Directivas 2008/48/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010 (DO L 60 de 28.2.2014, p. 34).

[54] Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (DO L 26 de 2.2.2016, p. 19).

Dichas autoridades competentes deben disponer de todas las facultades previstas en el presente Reglamento y en el Reglamento (UE) 2019/1020 para hacer cumplir los requisitos y las obligaciones del presente Reglamento, incluidas las facultades para llevar a cabo actividades de vigilancia del mercado a posteriori que puedan integrarse, según proceda, en sus mecanismos y procedimientos de supervisión existentes en virtud de la legislación pertinente de la Unión en materia de servicios financieros. Conviene prever que, cuando actúen como autoridades de vigilancia del mercado en virtud del presente Reglamento, las autoridades nacionales responsables de la supervisión de las entidades de crédito reguladas con arreglo a la Directiva 2013/36/UE, que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) nº 1024/201355 del Consejo, comuniquen sin demora al Banco Central Europeo toda información detectada en el curso de sus actividades de vigilancia del mercado que pueda ser de interés potencial para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

---

55 Reglamento (UE) nº 1024/2013 del Consejo, de 15 de octubre de 2013, por el que se confieren funciones específicas al Banco Central Europeo en relación con las políticas relativas a la supervisión prudencial de las entidades de crédito (DO L 287 de 29.10.2013,

p. 63).

Para reforzar aún más la coherencia entre el presente Reglamento y las normas aplicables a las entidades de crédito reguladas en virtud de la Directiva 2013/36/UE, conviene también integrar

▌ algunas de las obligaciones de procedimiento de los proveedores en relación con la gestión de riesgos, la supervisión posterior a la comercialización y la documentación en las obligaciones y procedimientos existentes en virtud de la Directiva 2013/36/UE. A fin de evitar solapamientos, también deben preverse excepciones limitadas en relación con el sistema de gestión de la calidad de los proveedores y la obligación de supervisión impuesta a ***los implantadores*** de sistemas de IA de alto riesgo en la medida en que se apliquen a las entidades de crédito reguladas por la Directiva 2013/36/UE. ***El mismo régimen debe aplicarse a las empresas de seguros y de reaseguros y a las sociedades de cartera de seguros con arreglo a la Directiva 2009/138/CE y a los intermediarios de seguros con arreglo a la Directiva (UE) 2016/97 y a otros tipos de entidades financieras sujetas a requisitos en materia de gobernanza interna, disposiciones o procesos establecidos de conformidad con la legislación pertinente de la Unión sobre servicios financieros para garantizar la coherencia y la igualdad de trato en el sector financiero.***

(159) Cada autoridad de vigilancia del mercado para los sistemas de IA de alto riesgo en el ámbito de la biometría, enumerados en un anexo del presente Reglamento, en la medida en que dichos sistemas se utilicen a efectos de la aplicación de la ley, la gestión de la migración, el asilo y el control de fronteras, o la administración de justicia y los procesos democráticos, debe tener poderes efectivos de investigación y corrección, incluida al menos la facultad de obtener acceso a todos los datos personales que se estén tratando y a toda la información necesaria para el desempeño de sus funciones. Las autoridades de vigilancia del mercado deben poder ejercer sus poderes actuando con total independencia. Cualquier limitación de su acceso a datos operativos sensibles en virtud del presente Reglamento debe entenderse sin perjuicio de las competencias que les confiere la Directiva (UE) 2016/680. Ninguna exclusión sobre la divulgación de datos a las autoridades nacionales de protección de datos en virtud del presente Reglamento debe afectar a las competencias actuales o futuras de dichas autoridades más allá del ámbito de aplicación del presente Reglamento.

(160) Las autoridades de vigilancia del mercado de los Estados miembros y la Comisión deben poder proponer actividades conjuntas, incluidas investigaciones conjuntas, que lleven a cabo las autoridades de vigilancia del mercado o las autoridades de vigilancia del mercado conjuntamente con la Comisión, que tengan por objeto promover el cumplimiento, detectar el incumplimiento, aumentar la sensibilización y proporcionar orientación en relación con el presente Reglamento con respecto a categorías específicas de sistemas de IA de alto riesgo que se considere que presentan un riesgo grave en dos o más Estados miembros. Las actividades conjuntas para promover el cumplimiento deben llevarse a cabo de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de Inteligencia Artificial debe prestar apoyo a la coordinación de las investigaciones conjuntas.

(161) Es necesario aclarar las responsabilidades y competencias a nivel de la Unión y nacional en lo que respecta a los sistemas de IA que se basan en modelos de IA de propósito general. Para evitar el solapamiento de competencias, cuando un sistema de IA se base en un modelo de IA de propósito general y el modelo y el sistema sean suministrados por el mismo proveedor, la supervisión debe tener lugar a nivel de la Unión a través de la Oficina de IA, que debe tener a tal efecto las competencias de una autoridad de vigilancia del mercado en el sentido del Reglamento (UE) 2019/1020. En todos los demás casos, las autoridades nacionales de vigilancia del mercado siguen siendo responsables de la supervisión de los sistemas de IA. Sin embargo, en el caso de los sistemas de IA de uso general que puedan ser utilizados directamente por los desplegadores para al menos un propósito clasificado como de alto riesgo, las autoridades de vigilancia del mercado deben cooperar con la Oficina de IA para llevar a cabo evaluaciones de cumplimiento e informar al Consejo y a otras autoridades de vigilancia del mercado en consecuencia. Además, las autoridades de vigilancia del mercado deben poder solicitar asistencia a la Oficina de IA cuando la autoridad de vigilancia del mercado no pueda concluir una investigación sobre un sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de propósito general en el que se basa el sistema de IA de alto riesgo. En tales casos, debe aplicarse mutatis mutandis el procedimiento relativo a la asistencia mutua en casos transfronterizos del capítulo VI del Reglamento (UE) 2019/1020.

(162) ***Para aprovechar al máximo la experiencia centralizada de la Unión y las sinergias a nivel de la Unión, las competencias de supervisión y ejecución de las obligaciones de los proveedores de modelos de IA de propósito general deben ser competencia de la Comisión. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de los poderes de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión basado en los Tratados. La Oficina de IA debe poder llevar a cabo todas las acciones necesarias para supervisar la aplicación efectiva del presente Reglamento en lo que respecta a los modelos de IA de propósito general. Debe poder investigar las posibles infracciones de las normas relativas a los proveedores de modelos de IA de propósito general tanto por iniciativa propia, a raíz de los resultados de sus actividades de supervisión, como a petición de las autoridades de vigilancia del mercado, en consonancia con las condiciones establecidas en el presente Reglamento. Para apoyar una supervisión eficaz de la Oficina de la IA, debe prever la posibilidad de que los proveedores intermedios presenten denuncias sobre posibles infracciones de las normas relativas a los proveedores de sistemas de IA de propósito general.***

(163) Con vistas a complementar los sistemas de gobernanza para los modelos de IA de propósito general, el panel científico debe apoyar las actividades de supervisión de la Oficina de IA y, en determinados casos, puede proporcionar alertas cualificadas a la Oficina de IA que desencadenen medidas de seguimiento, como investigaciones. Este debería ser el caso cuando el panel científico tenga motivos para sospechar que un modelo de IA de propósito general plantea un riesgo concreto e identificable a escala de la Unión. Además, este debe ser el caso cuando el panel científico tenga motivos para sospechar que un modelo de IA de propósito general cumple los criterios que llevarían a clasificarlo como modelo de IA de propósito general con riesgo sistémico. Para dotar al panel científico de la información necesaria para el desempeño de esas tareas, debe existir un mecanismo por el que el panel científico pueda solicitar a la Comisión que requiera documentación o información de un proveedor.

(164) ***La Oficina de IA debe poder adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento de las obligaciones de los proveedores de modelos de IA de propósito general establecidas en el presente Reglamento. La Oficina de IA debe poder investigar posibles infracciones de conformidad con las competencias previstas en el presente Reglamento, incluida la solicitud de documentación e información, la realización de evaluaciones, así como la solicitud de medidas a los proveedores de modelos de IA de propósito general. En la realización de las evaluaciones, con el fin de recurrir a expertos independientes, la Oficina de IA debe poder contar con la participación de expertos independientes para que lleven a cabo las evaluaciones en su nombre. El cumplimiento de las obligaciones debe poder exigirse, entre otras cosas, solicitando la adopción de medidas adecuadas, incluidas medidas de mitigación del riesgo en caso de riesgos sistémicos identificados, así como la restricción de la comercialización, la retirada o la recuperación del modelo. Como salvaguardia, cuando sea necesario más allá de los derechos procedimentales previstos en el presente Reglamento, los proveedores de modelos de IA de propósito general deben tener los derechos procedimentales previstos en el artículo 18 del Reglamento (UE) 2019/1020, que deben aplicarse mutatis mutandis, sin perjuicio de los derechos procedimentales más específicos previstos en el presente Reglamento.***

(165) El desarrollo de sistemas de IA distintos de los sistemas de IA de alto riesgo de conformidad con los requisitos del presente Reglamento puede dar lugar a una mayor adopción de IA ***ética y*** fiable en la Unión. Debe alentarse a los proveedores de sistemas de IA que no sean de alto riesgo a crear códigos de conducta***, incluidos los mecanismos de gobernanza conexos,*** destinados a fomentar la aplicación voluntaria de ***algunos o todos los*** requisitos obligatorios aplicables a los sistemas de IA de alto riesgo***, adaptados a la luz de la finalidad prevista de los sistemas y del menor riesgo que entrañan y teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector, como las tarjetas de modelo y de datos***. También debe alentarse a los proveedores ***y, en su caso, a los implantadores de todos los sistemas de IA, de alto riesgo o no, y modelos de IA*** a que apliquen de forma voluntaria requisitos adicionales relacionados, por ejemplo, con los ***elementos de las Directrices éticas de la Unión para una IA digna de confianza, la*** sostenibilidad medioambiental, ***las medidas de alfabetización en materia de IA, el diseño inclusivo y diverso y el desarrollo de sistemas de IA, incluida la atención a las personas vulnerables y la*** accesibilidad para las personas con discapacidad, la participación de las partes ***interesadas con la implicación, según proceda, de las partes interesadas pertinentes, como las empresas y las organizaciones de la sociedad civil, el mundo académico, las organizaciones de investigación, los sindicatos y la organización de protección de los consumidores***, en el diseño y desarrollo de los sistemas de IA, y la diversidad de los equipos de desarrollo***, incluido el equilibrio de género. Para garantizar la eficacia de los códigos de conducta voluntarios, deben basarse en objetivos claros e indicadores clave de rendimiento para medir la consecución de dichos objetivos. También deben desarrollarse de forma inclusiva, según proceda, con la participación de las partes interesadas pertinentes, como las organizaciones empresariales y de la sociedad civil, el mundo académico, las organizaciones de investigación, los sindicatos y las organizaciones de protección de los consumidores***. La Comisión podrá desarrollar iniciativas, incluso de carácter sectorial, para facilitar la reducción de las barreras técnicas que dificultan el intercambio transfronterizo de datos para el desarrollo de la IA, incluidas las relativas a la infraestructura de acceso a los datos y a la interoperabilidad semántica y técnica de los distintos tipos de datos.

(166) Es importante que los sistemas de IA relacionados con productos que no sean de alto riesgo con arreglo al presente Reglamento y que, por tanto, no estén obligados a cumplir los requisitos establecidos ***para los sistemas de IA de alto riesgo*** sean, no obstante, seguros cuando se comercialicen o se pongan en servicio. Para contribuir a este objetivo, se aplicaría como red de seguridad ***el Reglamento (UE) 2023/988*** del Parlamento Europeo y del **Consejo56**.

(167) Con el fin de garantizar una cooperación fiable y constructiva de las autoridades competentes a escala de la Unión y nacional, todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos obtenidos en el desempeño de sus funciones***, de conformidad con el Derecho de la Unión o nacional***. ***Deben llevar a cabo sus tareas y actividades de manera que se protejan, en particular, los derechos de propiedad intelectual, la información empresarial confidencial y los secretos comerciales, la aplicación efectiva del presente Reglamento, los intereses de la seguridad pública y nacional, la integridad de los procedimientos penales y administrativos y la integridad de la información clasificada.***

---

56 ***Reglamento (UE) 2023/988*** del Parlamento Europeo y del Consejo, de ***10 de mayo de 2023***, relativo a la seguridad general de los productos***, por el que se modifican el Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (DO L 135 de***

23.5.2023, p. 1).

(168) ***El cumplimiento del presente Reglamento debe poder exigirse mediante la imposición de sanciones y otras medidas coercitivas. Los*** Estados miembros deben adoptar todas las medidas necesarias para garantizar la aplicación de las disposiciones del presente Reglamento, en particular mediante el establecimiento de sanciones efectivas, proporcionadas y disuasorias en caso de infracción***, incluso en relación con el principio ne bis in idem. Con el fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, deben establecerse los límites máximos para la fijación de las multas administrativas*** por determinadas infracciones específicas***. Al evaluar el importe de las multas, los Estados miembros*** deben tener en cuenta***, en cada caso concreto, todas las circunstancias pertinentes de la situación específica, prestando la debida atención, en particular, a la naturaleza, gravedad y duración de la infracción y de sus consecuencias, así como al tamaño del proveedor, en particular si se trata de una PYME, incluida una empresa de nueva creación***. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas a las instituciones, agencias y organismos de la Unión que entren en el ámbito de aplicación del presente Reglamento.

(169) El cumplimiento de las obligaciones impuestas a los proveedores de modelos de IA de propósito general en virtud del presente Reglamento debe exigirse, entre otras cosas, mediante multas. A tal fin, también deben establecerse niveles adecuados de multas por incumplimiento de dichas obligaciones, incluido el incumplimiento de las medidas solicitadas por la Comisión de conformidad con el presente Reglamento, sujetas a plazos de prescripción adecuados de conformidad con el principio de proporcionalidad. Todas las decisiones adoptadas por la Comisión en virtud del presente Reglamento están sujetas al control del Tribunal de Justicia de la Unión Europea de conformidad con el TFUE.

(170) El Derecho de la Unión y los Derechos nacionales ya ofrecen vías de recurso efectivas a las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA. Sin perjuicio de estos recursos, cualquier persona física o jurídica que tenga motivos para considerar que se ha infringido el presente Reglamento debe tener derecho a presentar una denuncia ante la autoridad de vigilancia del mercado pertinente.

(171) Las personas afectadas deben tener derecho a obtener una explicación cuando la decisión de un responsable del despliegue se base principalmente en los resultados de determinados sistemas de alto riesgo incluidos en el ámbito de aplicación del presente Reglamento y cuando dicha decisión produzca efectos jurídicos o afecte significativamente de manera similar a dichas personas de un modo que estas consideren que repercute negativamente en su salud, su seguridad o sus derechos fundamentales. Dicha explicación debe ser clara y significativa y proporcionar una base sobre la que las personas afectadas puedan ejercer sus derechos. El derecho a obtener una explicación no debe aplicarse al uso de sistemas de IA para los que se deriven excepciones o restricciones del Derecho de la Unión o nacional, y sólo debe aplicarse en la medida en que este derecho no esté ya previsto en el Derecho de la Unión.

(172) Las personas que actúen como denunciantes de infracciones del presente Reglamento deben estar protegidas por el Derecho de la Unión. Por consiguiente, la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo[57] debe aplicarse a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien dichas infracciones.

---

57 Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de

2019, relativa a la protección de las personas que denuncian infracciones del Derecho de la Unión (DO L 305 de 26.11.2019, p. 17).

(173) A fin de garantizar que el marco reglamentario pueda adaptarse en caso necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE con objeto de modificar las condiciones en las que un sistema de IA no se considerará de alto riesgo, la lista de sistemas de IA de alto riesgo, las disposiciones relativas a la documentación técnica, el contenido de la declaración UE de conformidad, las disposiciones relativas a los procedimientos de evaluación de la conformidad, las disposiciones por las que se establecen los sistemas de IA de alto riesgo a los que debe aplicarse el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica***, el umbral, los puntos de referencia y los indicadores, incluso completando dichos puntos de referencia e indicadores, en las normas para la clasificación de los modelos de IA de propósito general con riesgo sistémico, los criterios para la designación de los modelos de IA de propósito general con riesgo sistémico, la documentación técnica para los proveedores de modelos de IA de propósito general y la información de transparencia para los proveedores de modelos de IA de propósito general***. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante sus trabajos preparatorios, incluso a nivel de expertos, y que dichas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 "Legislar mejor "[58]. En particular, para garantizar la igualdad de participación en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben todos los documentos al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupan de la preparación de los actos delegados.

[58] DO L 123 de 12.5.2016, p. 1.

(174) ***Habida cuenta de la rápida evolución tecnológica y de los conocimientos técnicos necesarios para la aplicación efectiva del presente Reglamento, la Comisión debe evaluar y revisar el presente Reglamento a más tardar ... [cinco años a partir de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, cada cuatro años, e informar al Parlamento Europeo y al Consejo. Además, teniendo en cuenta las implicaciones para el ámbito de aplicación del presente Reglamento, la Comisión debe llevar a cabo una evaluación de la necesidad de modificar la lista de sistemas de IA de alto riesgo y la lista de prácticas prohibidas una vez al año. Por otra parte, a más tardar dos años después de la entrada en vigor y posteriormente cada cuatro años, la Comisión debe evaluar e informar al Parlamento Europeo y al Consejo sobre la necesidad de modificar la lista de ámbitos de alto riesgo que figura en el anexo del presente Reglamento, los sistemas de IA incluidos en el ámbito de aplicación de las obligaciones de transparencia, la eficacia del sistema de supervisión y gobernanza y los avances en la elaboración de productos de normalización sobre el desarrollo energéticamente eficiente de modelos de IA de propósito general, incluida la necesidad de nuevas medidas o acciones. Por último, a más tardar ... [cuatro años después de la entrada en vigor del presente Reglamento] y posteriormente cada tres años, la Comisión debe evaluar el impacto y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos previstos para los sistemas de IA de alto riesgo en el caso de los sistemas de IA distintos de los sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para dichos sistemas de IA.***

(175) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del **Consejo59**.

(176) Dado que el objetivo del presente Reglamento, a saber, mejorar el funcionamiento del mercado interior y promover la adopción de la IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta, incluida la democracia, el Estado de Derecho y la protección del medio ambiente contra los efectos nocivos de los sistemas de IA en la Unión y apoyando la innovación, no puede ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

---

59 Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control, por parte de los Estados miembros, del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(177) Con el fin de garantizar la seguridad jurídica, asegurar un período de adaptación adecuado para los operadores y evitar perturbaciones en el mercado, entre otras cosas garantizando la continuidad del uso de los sistemas de IA, conviene que el presente Reglamento se aplique a los sistemas de IA de alto riesgo que se hayan comercializado o puesto en servicio antes de la fecha general de aplicación del mismo, únicamente si, a partir de esa fecha, dichos sistemas son objeto de cambios significativos en su diseño o finalidad prevista. Conviene aclarar que, a este respecto, el concepto de cambio significativo debe entenderse como equivalente en sustancia a la noción de modificación sustancial, que se utiliza únicamente en relación con los sistemas de IA de alto riesgo con arreglo al presente Reglamento. Con carácter excepcional y a la luz de la responsabilidad pública, los operadores de sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en un anexo del presente Reglamento y los operadores de sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas deben, respectivamente, adoptar las medidas necesarias para cumplir los requisitos del presente Reglamento antes de finales de 2030 y antes de seis años después de su entrada en vigor.

(178) Se anima a los proveedores de sistemas de IA de alto riesgo a que empiecen a cumplir, de forma voluntaria, las obligaciones pertinentes del presente Reglamento ya durante el período transitorio.

(179) El presente Reglamento debe aplicarse a partir de ... [dos años desde la fecha de entrada en vigor del presente Reglamento]. Sin embargo, teniendo en cuenta ***el riesgo inaceptable asociado al uso de la IA en determinadas formas, las prohibiciones deben aplicarse ya a partir de ... [seis meses desde la fecha de entrada en vigor del presente Reglamento]. Si bien el pleno efecto de dichas prohibiciones se produce con el establecimiento de la gobernanza y la aplicación del presente Reglamento, anticipar la aplicación de las prohibiciones es importante para tener en cuenta los riesgos inaceptables y para que tengan efecto en otros procedimientos, como en el Derecho civil. Además,*** la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad debe ser operativa antes de esa fecha, por lo que las disposiciones sobre los organismos notificados y la estructura de gobernanza deben aplicarse a partir de ... [***12*** meses después de la ***fecha de entrada en vigor del presente Reglamento***]. ***Dado el rápido ritmo de los avances tecnológicos y la adopción de modelos de IA de propósito general, las obligaciones para los proveedores de modelos de IA de propósito general deben aplicarse a partir de ... [12 meses a partir de la fecha de entrada en vigor del presente Reglamento]. Los códigos de buenas prácticas deben estar listos para ... [9 meses a partir de la fecha de entrada en vigor*** del presente Reglamento] ***para que los proveedores puedan demostrar su cumplimiento a tiempo. La Oficina de AI debe velar por que las normas y procedimientos de clasificación se actualicen a la luz de los avances tecnológicos.*** Además, los Estados miembros deben establecer y notificar a la Comisión el régimen de sanciones, incluidas las multas administrativas, y velar por su correcta y eficaz aplicación en la fecha de entrada en vigor del presente Reglamento. Por consiguiente, las disposiciones sobre sanciones deben aplicarse a partir de ... [12 meses después de la fecha de entrada en vigor del presente Reglamento].

(180) El Supervisor Europeo de Protección de Datos y el Consejo Europeo de Protección de Datos fueron consultados de conformidad con el artículo 42, apartados 1 y 2, del Reglamento (UE) 2018/1725 y emitieron su dictamen conjunto el ▌ ***18 de junio de 2021***,

HAN ADOPTADO ESTE REGLAMENTO:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1

Objeto

1. ***El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de la inteligencia artificial (IA) centrada en el ser humano y digna de confianza, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales, incluida la democracia, el Estado de Derecho y la protección del medio ambiente, contra los efectos nocivos de los sistemas de inteligencia artificial*** (sistemas de IA) ***en la Unión, y apoyar la innovación.***

2. Este Reglamento establece:

(a) normas armonizadas para la comercialización, la puesta en servicio y el uso de los sistemas de IA en la Unión;

(b) prohibiciones de determinadas prácticas de IA;

(c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;

(d) normas de transparencia armonizadas para ***determinados*** sistemas de IA***;***

(e) normas armonizadas para la comercialización de modelos de IA de uso general;

(f) normas sobre supervisión del mercado***, gobernanza de la vigilancia del mercado y ejecución;***

(g) Medidas de apoyo a la innovación, con especial atención a las PYME, incluidas las de nueva creación.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica a:

(a) proveedores que comercialicen o ***pongan en*** servicio sistemas de IA ***o comercialicen modelos de IA de uso general*** en la Unión, con independencia de que dichos proveedores estén establecidos ***o ubicados*** en la Unión o en un tercer país;

(b) ***desplegadores*** de sistemas de IA ***que tengan su lugar de establecimiento o estén*** situados en la Unión;

(c) proveedores e ***implantadores*** de sistemas de IA que ***tengan su lugar de establecimiento o*** estén situados en un tercer país, cuando el producto generado por el sistema de IA se utilice en la Unión;

(d) importadores y distribuidores de sistemas de IA;

(e) fabricantes de productos que comercializan o ponen en servicio un sistema de IA junto con su producto y bajo su propio nombre o marca;

(f) representantes autorizados de proveedores no establecidos en la Unión;

(g) afectados que se encuentren en la Unión.

2. Para ▌ los sistemas de IA ***clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y***

(2) en relación con los productos ***cubiertos por la legislación de armonización de la Unión enumerada en la sección B del anexo I,*** sólo se aplica el artículo 112***. El artículo 57 se aplica únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo con arreglo al presente Reglamento se hayan integrado en dicha legislación de armonización de la Unión.***

▌

3. ***El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado la realización de tareas en relación con dichas competencias.***

El presente Reglamento no se aplica a los sistemas de IA ***cuando y en la medida en que se comercialicen, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo dichas actividades.***

El presente Reglamento no se aplicará a los sistemas de IA que no se comercialicen o pongan en servicio en la Unión, cuando el producto se utilice en la Unión exclusivamente con fines militares***, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo dichas actividades***.

4. El presente Reglamento no se aplica a las autoridades públicas de un tercer país ni a las organizaciones internacionales incluidas en el ámbito de aplicación del presente Reglamento con arreglo al apartado 1, cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de la ***cooperación*** internacional ***o de*** acuerdos de cooperación policial y judicial con la Unión o con uno o varios Estados miembros***, siempre que dicho tercer país u organización internacional ofrezca garantías adecuadas con respecto a la protección de los derechos y libertades fundamentales de las personas.***

5. El presente Reglamento no afectará a la aplicación de las disposiciones sobre la responsabilidad de los prestadores de servicios de intermediación establecidas en el capítulo II del Reglamento (UE) 2022/2065.

6. El presente Reglamento no se aplica a los sistemas de IA o a los modelos de IA, incluidos sus resultados, específicamente desarrollados y puestos en servicio con el único fin de la investigación y el desarrollo científicos.

7. El Derecho de la Unión en materia de protección de datos personales, intimidad y confidencialidad de las comunicaciones se aplica a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725, ni a las Directivas 2002/58/CE o (UE) 2016/680, sin perjuicio de lo dispuesto en el artículo 10, apartado 5, y en el artículo 59 del presente Reglamento.

8. El presente Reglamento no se aplica a ninguna actividad de investigación, ensayo o desarrollo relativa a sistemas o modelos de IA antes de su comercialización o puesta en servicio. Dichas actividades se llevarán a cabo de conformidad con el Derecho aplicable de la Unión. Las pruebas en condiciones reales no estarán cubiertas por dicha exclusión.

9. ***El presente Reglamento se entiende sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relacionados con la protección de los consumidores y la seguridad de los productos.***

10. ***El presente Reglamento no se aplica a las obligaciones de los implantadores que sean personas físicas que utilicen sistemas de IA en el curso de una actividad no profesional puramente personal.***

11. ***El presente Reglamento no se opone a que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas más favorables para los trabajadores en lo que respecta a la protección de sus derechos en relación con la utilización de sistemas de IA por parte de los empresarios, ni a que fomenten o permitan la aplicación de convenios colectivos más favorables para los trabajadores.***

12. ***El presente Reglamento se aplica a los sistemas de IA liberados bajo licencias libres y de código abierto, a menos que se comercialicen o se pongan en servicio como sistemas de IA de alto riesgo o como un sistema de IA que entre en el ámbito de aplicación de los artículos 5 o 50.***

Artículo 3

Definicione

s

A efectos del presente Reglamento, se entenderá por

(1) sistema de ***IA"****: un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía, que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe*, ***cómo*** generar salidas tales como ***predicciones, contenidos***, recomendaciones o decisiones ***que pueden influir en*** entornos ***físicos o virtuales***;

(2) riesgo": la combinación de la probabilidad de que se produzca un daño y la gravedad de ese daño;

(3) proveedor": una persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolle un sistema de IA o un ***modelo de IA de propósito general o*** que haga ***desarrollar*** un sistema de IA ***o un modelo de IA de propósito general y lo*** comercialice o ***ponga*** en servicio ***el sistema de IA*** bajo su propio nombre o marca, ya sea a título oneroso o gratuito;

(4) "***implantador"***: una persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de IA bajo su autoridad ▌ excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional;

(5) representante autorizado": una persona física o jurídica ***situada o*** establecida en la Unión que ha recibido ***y aceptado*** un mandato escrito de un proveedor de un sistema de IA ***o de un modelo de IA de propósito general*** para, respectivamente, ejecutar y llevar a cabo en su nombre las obligaciones y procedimientos establecidos por el presente Reglamento;

(6) "importador": una persona física o jurídica ***situada o*** establecida en la Unión que comercializa ▌ un sistema de IA que lleva el nombre o la marca comercial de una persona física o jurídica establecida en un tercer país;

(7) "distribuidor": una persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que comercializa un sistema de IA en el mercado de la Unión ▌ ;

(8) operador": proveedor, ***fabricante de productos, implantador***, representante autorizado, importador ***o*** distribuidor;

(9) comercialización": la primera puesta a disposición en el mercado de la Unión de un sistema de IA ***o de un modelo de IA de propósito general***;

(10) puesta a disposición en el mercado": el suministro de un sistema de IA ***o de un modelo de IA de uso general*** para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, ya sea a cambio de una remuneración o de forma gratuita;

(11) "puesta en servicio": el suministro de un sistema de IA por parte del proveedor para su primer uso directamente al ***implantador*** o para uso propio ***en*** la Unión ▌ para los fines previstos;

(12) finalidad prevista": el uso al que el proveedor destina un sistema de IA, incluidos el contexto y las condiciones de uso específicos, tal como se especifica en la información facilitada por el proveedor en las instrucciones de uso, el material promocional o de venta y las declaraciones, así como en la documentación técnica;

(13) uso indebido razonablemente previsible": el uso de un sistema de IA de forma no conforme con su finalidad prevista, pero que puede resultar de un comportamiento humano razonablemente previsible o de la interacción con otros sistemas***, incluidos otros sistemas de IA***;

(14) Componente de seguridad": componente de un producto o de un sistema que cumple una función de seguridad para dicho producto o sistema**,** o cuyo fallo o mal funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes;

(15) instrucciones de uso": la información facilitada por el proveedor para informar al usuario, en particular, sobre la finalidad prevista y el uso adecuado de un sistema de IA ▌;

(16) retirada de un sistema de IA": cualquier medida destinada a lograr el retorno al proveedor ***o a poner fuera de servicio o inhabilitar el uso*** de un sistema de IA puesto a disposición de los ***implantadores***;

(17) retirada de un sistema de IA": cualquier medida destinada a impedir que ***un sistema de IA de la cadena de suministro se comercialice***;

(18) rendimiento de un sistema de inteligencia artificial": la capacidad de un sistema de inteligencia artificial para alcanzar el objetivo previsto;

(19) autoridad notificante": la autoridad nacional responsable de establecer y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión;

(20) evaluación de la conformidad": el proceso de ***demostrar*** si se han cumplido los requisitos establecidos en la sección 2 del capítulo II relativos a ***un*** sistema de IA ***de alto riesgo***;

(21) organismo de evaluación de la conformidad": un organismo que realiza actividades de evaluación de la conformidad por terceros, incluidos los ensayos, la certificación y la inspección;

(22) organismo notificado": un organismo de evaluación de la conformidad ***notificado con*** arreglo al presente Reglamento y a otras disposiciones pertinentes de la legislación de armonización de la Unión enumeradas en la sección B del anexo I;

(23) modificación sustancial": un cambio en un sistema de IA ***después de*** su comercialización o puesta en servicio que ***no esté previsto o planificado en la evaluación inicial de la conformidad realizada por el proveedor y como resultado del cual se vea afectada*** la conformidad del sistema de IA con los requisitos establecidos en la sección 2 del capítulo II o se produzca una modificación de la finalidad prevista para la que se ha evaluado el sistema de IA;

(24) marcado CE": un marcado por el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo II, sección 2, y con otra legislación de armonización de la Unión aplicable enumerada en el anexo I, que prevé su colocación;

(25) "***sistema de*** seguimiento poscomercialización": todas las actividades llevadas a cabo por los proveedores de sistemas de IA para ▌ recopilar y revisar la experiencia adquirida con el uso de los sistemas de IA que comercializan o ponen en servicio con el fin de detectar cualquier necesidad de aplicar inmediatamente las medidas correctoras o preventivas necesarias;

(26) "autoridad de vigilancia del mercado": la autoridad nacional que lleva a cabo las actividades y adopta las medidas de conformidad con el Reglamento (UE) 2019/1020;

(27) "norma armonizada": una norma armonizada tal como se define en el artículo 2, apartado 1, letra c), del Reglamento (UE) no 1025/2012;

(28) "***especificación*** común": un ***conjunto de especificaciones técnicas, tal como se definen en el artículo 2, punto 4, del Reglamento (UE) no 1025/2012, que proporciona*** medios para ▌cumplir determinados requisitos ▌establecidos en virtud del presente Reglamento;

(29) datos de entrenamiento": datos utilizados para entrenar un sistema de IA mediante el ajuste de sus parámetros aprendibles ▌;

(30) datos de validación": los datos utilizados para proporcionar una evaluación del sistema de IA entrenado y para ajustar sus parámetros no aprendibles y su proceso de aprendizaje con el fin, entre otras cosas, de evitar la ***adaptación insuficiente o*** excesiva;

(31) conjunto de datos de validación": conjunto de datos separado o parte del conjunto de datos de entrenamiento, ya sea como división fija o variable;

(32) datos de ensayo": los datos utilizados para proporcionar una evaluación independiente del sistema de IA a fin de confirmar el rendimiento esperado de dicho sistema antes de su comercialización o puesta en servicio;

(33) datos de entrada": los datos proporcionados a un sistema de IA o adquiridos directamente por éste, a partir de los cuales el sistema produce un resultado;

(34) datos biométricos": los datos personales resultantes de un tratamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona física, ▌ como las imágenes faciales o los datos dactiloscópicos;

(35) identificación biométrica": el reconocimiento automatizado de rasgos humanos físicos, fisiológicos, conductuales o psicológicos con el fin de establecer la identidad de una persona física mediante la comparación de datos biométricos de dicha persona con datos biométricos de individuos almacenados en una base de datos;

(36) verificación biométrica": la verificación automatizada y unívoca, incluida la autenticación, de la identidad de personas físicas mediante la comparación de sus datos biométricos con datos biométricos facilitados previamente;

(37) "categorías especiales de datos personales": las categorías de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725;

(38) datos operativos sensibles": los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos, cuya divulgación podría poner en peligro la integridad de los procedimientos penales;

(39) sistema de reconocimiento de emociones": un sistema de IA destinado a identificar o deducir emociones o intenciones de personas físicas a partir de sus datos biométricos;

(40) sistema de categorización biométrica": un sistema de IA destinado a asignar personas físicas a categorías específicas ***sobre la base de sus datos biométricos, a menos que sea auxiliar de otro servicio comercial y estrictamente necesario por razones técnicas objetivas***;

(41) "sistema de identificación biométrica a distancia": un sistema de IA destinado a identificar a personas físicas***, sin su participación activa, normalmente a*** distancia mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia ▌ ;

(42) sistema de identificación biométrica a distancia en tiempo real": un sistema de identificación biométrica a distancia en el que la captura de los datos biométricos, la comparación y la identificación se producen sin demora significativa y comprende no sólo la identificación instantánea, sino también demoras breves limitadas para evitar la elusión;

(43) sistema de identificación biométrica a distancia posterior": un sistema de identificación biométrica a distancia distinto de un sistema de identificación biométrica a distancia en tiempo real;

(44) espacio de acceso público": cualquier lugar físico ***de propiedad pública o privada*** accesible a ***un número indeterminado de personas físicas***, con independencia de que puedan aplicarse determinadas condiciones de acceso ***y de las posibles restricciones de capacidad***;

(45) autoridad encargada de hacer cumplir la ley

(a) cualquier autoridad pública competente en materia de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública; o

(b) cualquier otro organismo o entidad al que la legislación de un Estado miembro encomiende el ejercicio de la autoridad pública y de los poderes públicos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la salvaguardia y la prevención de amenazas para la seguridad pública;

(46) aplicación de la ley": actividades llevadas a cabo por las autoridades policiales y judiciales ***o en su nombre*** para la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública;

(47) ***Oficina de Inteligencia Artificial": la función de la Comisión de contribuir a la aplicación, el seguimiento y la supervisión de los sistemas de inteligencia artificial y la gobernanza de la inteligencia artificial llevada a cabo por la Oficina Europea de Inteligencia Artificial creada por Decisión de la Comisión de 24.1.2024; las referencias del presente Reglamento a la Oficina de Inteligencia Artificial se entenderán hechas a la Comisión;***

(48) autoridad nacional competente": ***una*** autoridad notificante o una autoridad de vigilancia del mercado***;***;

(49) Incidente grave": un incidente ***o un mal funcionamiento de un sistema de IA que provoque directa o indirectamente*** cualquiera de las siguientes situaciones:

(a) la muerte de una persona o un daño grave para su salud***;***

(b) una perturbación grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas.

(c) el incumplimiento ***de las obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales;***

(d) daños graves a la propiedad o al medio ambiente;

(50) "datos personales": los datos personales definidos en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

(51) "datos no personales": datos distintos de los datos personales definidos en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

(52) "elaboración de perfiles": la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679 o, en el caso de las autoridades policiales y judiciales, tal como se define en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o, en el caso de las instituciones, órganos u organismos de la Unión, tal como se define en el artículo 3, punto 5, del Reglamento (UE) 2018/1725;

(53) plan de ensayos en condiciones reales": documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, el seguimiento, la organización y la realización de los ensayos en condiciones reales;

(54) plan del sandbox": documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos de las actividades realizadas dentro del sandbox;

(55) recinto de seguridad reglamentario de la IA": un marco controlado establecido por una autoridad competente que ofrece a los proveedores o posibles proveedores de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en su caso en condiciones reales, un sistema de IA innovador, con arreglo a un plan de recinto de seguridad durante un tiempo limitado bajo supervisión reglamentaria;

(56) Por "alfabetización en IA" se entienden las capacidades, los conocimientos y la comprensión que permiten a los proveedores, a los implantadores y a las personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, realizar una implantación informada de los sistemas de IA, así como adquirir conciencia de las oportunidades y los riesgos de la IA y de los posibles daños que puede causar;

(57) ensayo en condiciones reales": el ensayo temporal de un sistema de IA para su finalidad prevista en condiciones reales fuera de un laboratorio o de un entorno simulado de otro modo, con vistas a recopilar datos fiables y sólidos y a evaluar y verificar la conformidad del sistema de IA con los requisitos del presente Reglamento, y no se considera comercialización ni puesta en servicio del sistema de IA en el sentido del presente Reglamento, siempre que se cumplan todas las condiciones establecidas en los artículos 57 o 60;

(58) sujeto", a efectos de las pruebas en condiciones reales, una persona física que participa en las pruebas en condiciones reales;

(59) consentimiento informado": la manifestación libre, específica, inequívoca y voluntaria de un sujeto de su voluntad de participar en un ensayo concreto en condiciones reales, tras haber sido informado de todos los aspectos del ensayo que son relevantes para la decisión del sujeto de participar;

(60) falsificación profunda": contenido de imagen, audio o vídeo generado o manipulado por IA que se asemeja a personas, objetos, lugares u otras entidades o acontecimientos existentes y que a una persona le parecería falsamente auténtico o veraz;

(61) infracción generalizada": cualquier acción u omisión contraria al Derecho de la Unión que proteja los intereses de las personas, que:

(a) haya perjudicado o pueda perjudicar los intereses colectivos de personas físicas residentes en al menos dos Estados miembros distintos del Estado miembro en el que:

(i) se originó o tuvo lugar el acto o la omisión;

(ii) se encuentre o esté establecido el proveedor de que se trate o, en su caso, su representante autorizado; o

(iii) cuando la infracción sea cometida por el ejecutor;

(b) haya causado, cause o pueda causar un perjuicio a los intereses colectivos de los particulares y presente características comunes, como la misma práctica ilícita o el mismo interés vulnerado, y se produzca de forma concurrente, cometida por el mismo operador, en al menos tres Estados miembros;

(62) infraestructura crítica": la infraestructura crítica definida en el artículo 2, punto (4), de la Directiva (UE) 2022/2557;

(63) modelo de IA de propósito general": un modelo de IA, incluso cuando dicho modelo de IA se entrene con una gran cantidad de datos utilizando la autosupervisión a escala, que muestre una generalidad significativa y sea capaz de realizar de forma competente una amplia gama de tareas distintas, independientemente de la forma en que se comercialice el modelo, y que pueda integrarse en una variedad de sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilicen para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización;

(64) Por "capacidades de alto impacto" se entienden las capacidades que igualan o superan las registradas en los modelos de IA de propósito general más avanzados;

(65) riesgo sistémico": un riesgo específico de las capacidades de alto impacto de los modelos de IA de propósito general, que tiene un impacto significativo en el mercado de la Unión debido a su alcance, o debido a efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que pueden propagarse a escala en toda la cadena de valor;

(66) sistema de IA de propósito general": un sistema de IA basado en un modelo de IA de propósito general, capaz de servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

(67) operación en coma flotante" o "FLOP": cualquier operación matemática o asignación que implique números en coma flotante, que son un subconjunto de los números reales típicamente representados en los ordenadores por un número entero de precisión fija escalado por un exponente entero de base fija;

(68) proveedor intermedio": un proveedor de un sistema de IA, incluido un sistema de IA de propósito general, que integra un modelo de IA, independientemente de que el modelo sea proporcionado por ellos mismos e integrado verticalmente o proporcionado por otra entidad sobre la base de relaciones contractuales.

Artículo 4

Alfabetizac

ión en IA

Los proveedores e implantadores de sistemas de inteligencia artificial adoptarán medidas para garantizar, en la medida de lo posible, un nivel suficiente de conocimientos de inteligencia artificial de su personal y de otras personas que se ocupen del funcionamiento y uso de los sistemas de inteligencia artificial en su nombre, teniendo en cuenta sus conocimientos técnicos, experiencia, educación y formación y el contexto en el que vayan a utilizarse los sistemas de inteligencia artificial, y considerando las personas o grupos de personas sobre los que vayan a utilizarse los sistemas de inteligencia artificial.

CAPÍTULO II
PRÁCTICAS DE INTELIGENCIA ARTIFICIAL PROHIBIDAS

Artículo 5

Prácticas de IA prohibidas

1. Quedan prohibidas las siguientes prácticas de IA:

   (a) la comercialización, la puesta en servicio o la utilización de un sistema de IA que utilice técnicas subliminales que escapen a la conciencia de una persona ***o técnicas deliberadamente manipuladoras o engañosas, con el objetivo o el efecto de distorsionar*** materialmente el comportamiento de una persona ***o de un grupo de personas, mermando sensiblemente su capacidad de tomar una decisión con conocimiento de causa, haciendo así que una persona tome una decisión que de otro modo no habría tomado,*** de forma que cause o pueda causar a esa persona***, a*** otra persona ***o a un grupo de personas un*** perjuicio importante;

(b) la puesta en el mercado, la puesta en servicio o el uso de un sistema de IA que explote cualquiera de las vulnerabilidades de una ***persona o de un*** grupo específico de personas debido a su edad, ***discapacidad o una situación social o económica específica, con el objetivo, o el efecto, de distorsionar*** materialmente el comportamiento de ***esa persona o de*** una persona perteneciente a ese grupo de manera que cause o sea ***razonablemente*** probable que cause a esa persona o a otra ***un daño significativo;***

(c) la puesta en el mercado, la puesta en servicio o la utilización de sistemas de IA ▌ con fines de evaluación o clasificación de ***personas físicas o grupos de personas*** durante un determinado período de tiempo en función de su comportamiento social o de sus características personales o de personalidad conocidas***, deducidas*** o previstas, con la puntuación social que conduzca a una de las siguientes situaciones o a ambas:

(i) trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros de personas en contextos sociales que no guardan relación con los contextos en los que se generaron o recopilaron originalmente los datos;

(ii) trato perjudicial o desfavorable a determinadas personas físicas o ▌ grupos de personas injustificado o desproporcionado a su comportamiento social o a su gravedad;

(d) ***la comercialización, la puesta en servicio para este fin específico, o el uso de un sistema de IA para realizar evaluaciones de riesgo de personas físicas con el fin de evaluar o predecir la probabilidad de que una persona física cometa un delito, basándose únicamente en el perfil de una persona física o en la evaluación de sus rasgos y características de personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva, que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva;***

(e) ***la puesta en el mercado, la puesta en servicio con este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial a través de la extracción no selectiva de imágenes faciales de Internet o de grabaciones de CCTV;***

(f) la puesta en el mercado, la puesta en servicio con este fin específico o el uso de sistemas de IA para inferir emociones de una persona física en los ámbitos del lugar de trabajo y de las instituciones educativas, excepto cuando el uso del sistema de IA se destine a la puesta en el mercado o a la puesta en servicio por motivos médicos o de seguridad.

(g) ***la comercialización, la puesta en servicio con este fin específico, o el uso de sistemas de categorización biométrica que categoricen individualmente a personas físicas basándose en sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no cubre ningún etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basándose en datos biométricos o categorización de datos biométricos en el ámbito de la aplicación de la ley;***

(h) la utilización de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales, ▌ a menos y en la medida en que dicha utilización sea estrictamente necesaria para uno de los siguientes objetivos:

(i) la búsqueda selectiva de víctimas concretas ▌ de ***secuestros, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas*** desaparecidas***;***

(ii) la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas o ***una amenaza real y actual o real y previsible*** de atentado terrorista;

(iii) la ▌ localización ***o*** identificación ***de una persona sospechosa de haber cometido una infracción penal, con el fin de llevar a cabo*** una ***investigación*** penal***, el enjuiciamiento o la ejecución de una sanción penal por las infracciones contempladas en el anexo II*** y castigadas en el Estado miembro de que se trate con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos ***cuatro*** años;

▌

La letra h) del párrafo primero se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 para el tratamiento de datos biométricos con fines distintos de los policiales.

2. El uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales para cualquiera de los objetivos mencionados en el apartado 1, letra h***), se desplegará únicamente para los fines establecidos en el apartado 1, letra h), para confirmar la identidad de la persona a la que se dirige específicamente, y tendrá en cuenta*** los siguientes elementos:

(a) la naturaleza de la situación que da lugar a la posible utilización, en particular la gravedad, la probabilidad y la magnitud del perjuicio que se causaría si no se utilizara el sistema;

(b) las consecuencias de la utilización del sistema para los derechos y libertades de todas las personas afectadas, en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público a efectos de la aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra h), del presente artículo se ajustará a las salvaguardias y condiciones necesarias y proporcionadas en relación con el uso de ***conformidad con la legislación nacional que autorice su uso***, en particular en lo que se refiere a las limitaciones temporales, geográficas y personales. ***El uso del sistema de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público sólo se autorizará si la autoridad policial ha realizado una evaluación de impacto sobre los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, podrá iniciarse la utilización de tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.***

3. A efectos del apartado 1, letra h), y del apartado 2, cada ▌ utilización con fines policiales de un sistema de identificación biométrica a distancia "en tiempo real" en espacios de acceso público estará sujeta a una autorización previa concedida por una autoridad judicial o

▌ una autoridad administrativa independiente ***cuya decisión sea vinculante*** para el Estado miembro en el que vaya a tener lugar la utilización, expedida previa solicitud motivada y de conformidad con las disposiciones de Derecho interno a que se refiere el apartado 5. No obstante, en una situación de urgencia debidamente justificada, podrá iniciarse la utilización de dicho sistema sin autorización***, siempre que*** ésta ***se*** solicite ***sin demora indebida, a más tardar en un plazo de 24 horas. Si se deniega dicha autorización, se interrumpirá el uso con efecto inmediato y todos los datos, así como los resultados y productos de dicho uso, se desecharán y suprimirán inmediatamente***.

La autoridad judicial competente ***o una*** autoridad administrativa ***independiente cuya decisión sea vinculante*** concederá la autorización únicamente cuando esté convencida, sobre la base de pruebas objetivas o indicios claros que se le presenten, de que el uso del sistema de identificación biométrica a distancia "en tiempo real" de que se trate es necesario y proporcionado para alcanzar uno de los objetivos especificados en el apartado 1, letra h), tal como se identifica en la solicitud ***y, en particular, se limita a lo estrictamente necesario en cuanto al período de tiempo y al ámbito geográfico y personal.*** Al decidir sobre la solicitud***,*** dicha ***autoridad tendrá en cuenta*** los elementos mencionados en el apartado 2***. No podrá tomarse ninguna decisión que produzca un efecto jurídico adverso sobre una persona basándose únicamente en los resultados del sistema de identificación biométrica a distancia*** "en tiempo real"**.**

4. ***Sin perjuicio de lo dispuesto en el apartado 3, cada utilización de un sistema de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.***

5. 4. Un Estado miembro podrá decidir prever la posibilidad de autorizar total o parcialmente el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público a efectos de la aplicación de la ley dentro de los límites y en las condiciones enumerados en el apartado 1, letra h), y en los apartados 2 y 3. ▌ Los Estados miembros de ***que se trate establecerán*** en ***su*** Derecho nacional las normas detalladas necesarias para la solicitud, expedición y ejercicio de las autorizaciones a que se refiere el apartado 3, así como para su supervisión ***e información***. Dichas normas especificarán asimismo para cuáles de los objetivos enumerados en la letra h) del apartado 1, incluidos los delitos a que se refiere el inciso iii) de dicha letra h), puede autorizarse a las autoridades competentes a utilizar dichos sistemas con fines policiales. ***Los Estados miembros notificarán dichas normas a la Comisión a más tardar 30 días después de su adopción. Los Estados miembros podrán introducir, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica a distancia.***

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios accesibles al público con fines policiales de conformidad con el apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o por una autoridad administrativa independiente cuya decisión sea vinculante para las solicitudes de autorización de conformidad con el apartado 3 y su resultado.

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica a distancia en tiempo real en espacios de acceso público con fines policiales, basados en datos agregados en los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades policiales relacionadas.

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otra legislación de la Unión.

CAPÍTULO III
SISTEMAS DE AI DE ALTO RIESGO

Sección 1
Clasificación de los sistemas de IA como de alto riesgo

Artículo 6

Reglas de clasificación de los sistemas de IA de alto riesgo

1. Independientemente de que un sistema de IA se comercialice o se ponga en servicio independientemente de los productos contemplados en las letras a) y b), dicho sistema de IA se considerará de alto riesgo cuando se cumplan las dos condiciones siguientes:

   (a) el sistema de IA está destinado a utilizarse como componente de seguridad de un producto, o ***el sistema de IA*** es en sí mismo un producto, cubierto por la legislación de armonización de la Unión enumerada en el anexo I;

   (b) el producto cuyo componente de seguridad con ***arreglo a la letra a)*** es el sistema de IA, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad por terceros***, con*** vistas a la introducción en el mercado o la puesta en servicio de dicho producto con arreglo a la legislación de armonización de la Unión enumerada en el anexo I**.**

2. Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, se considerarán de alto riesgo los sistemas de IA a que se refiere el anexo III.

3. No obstante lo dispuesto en el apartado 2, un sistema de IA no se considerará de alto riesgo si no plantea un riesgo significativo de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas, incluso por no influir materialmente en el resultado de la toma de decisiones. Este será el caso cuando se cumplan una o varias de las siguientes condiciones:

(a) el sistema de IA está destinado a realizar una tarea procedimental limitada;

(b) el sistema de IA pretende mejorar el resultado de una actividad humana realizada previamente;

(c) el sistema de IA está destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores y no está destinado a sustituir o influir en la evaluación humana previamente completada, sin la debida revisión humana; o

(d) el sistema de IA está destinado a realizar una tarea preparatoria de una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero, un sistema de IA contemplado en el anexo III se considerará siempre de alto riesgo cuando el sistema de IA realice la elaboración de perfiles de personas físicas.

4. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo documentará su evaluación antes de que dicho sistema se comercialice o se ponga en servicio. Dicho proveedor estará sujeto a la obligación de registro establecida en
Artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

5. La Comisión, previa consulta a la Junta Europea de Inteligencia Artificial (la "Junta"), y a más tardar ... [18 meses a partir de la fecha de entrada en vigor del presente Reglamento], proporcionará directrices que especifiquen la aplicación práctica del presente artículo en consonancia con el artículo 96, junto con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA de alto riesgo y de no alto riesgo.

6. La Comisión adoptará actos delegados con arreglo al artículo 97 para modificar las condiciones establecidas en el apartado 3, párrafo primero, del presente artículo.

La Comisión podrá adoptar actos delegados de conformidad con el artículo 97 con el fin de añadir nuevas condiciones a las establecidas en el apartado 3, párrafo primero, o modificarlas, únicamente cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del anexo III pero no planteen un riesgo significativo de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas.

La Comisión adoptará actos delegados con arreglo al artículo 97 para suprimir cualquiera de las condiciones establecidas en el párrafo primero del apartado 3, cuando existan pruebas concretas y fiables de que ello es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales en la Unión.

Cualquier modificación de las condiciones establecidas en el párrafo primero del apartado 3 no disminuirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales en la Unión.

Al adoptar los actos delegados, la Comisión garantizará la coherencia con los actos delegados adoptados en virtud del artículo 7, apartado 1, y tendrá en cuenta la evolución del mercado y de la tecnología.

Artículo 7

Modificaciones del anexo III

1. La Comisión adoptará actos delegados de conformidad con el artículo 97 para ***modificar*** el anexo III añadiendo ***o modificando casos de uso de*** sistemas de IA de alto riesgo cuando se cumplan las dos condiciones siguientes:

   (a) los sistemas de IA están destinados a utilizarse en cualquiera de los ámbitos enumerados en el anexo III;

(b) los sistemas de IA plantean un riesgo de daño para ▌ la salud y la seguridad, o ***un impacto*** adverso en los derechos fundamentales, ***y ese riesgo es*** equivalente o mayor que el riesgo de daño o de impacto adverso que plantean los sistemas de IA de alto riesgo ya mencionados en el anexo III.

2. Al evaluar la condición prevista en la letra b) del apartado 1, la Comisión tendrá en cuenta los siguientes criterios:

(a) la finalidad prevista del sistema de IA;

(b) la medida en que se ha utilizado o es probable que se utilice un sistema de IA;

(c) la naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

(d) la medida en que el sistema de IA actúa de forma autónoma y la posibilidad de que un humano anule una decisión o unas recomendaciones que puedan provocar un daño potencial;

(e) la medida en que el uso de un sistema de IA ya ha causado daños a la salud y la seguridad***, ha tenido un*** impacto adverso en los derechos fundamentales o ha suscitado preocupaciones significativas en relación con la ***probabilidad*** de tales daños o impactos adversos, como demuestran, por ***ejemplo,*** informes o alegaciones documentadas presentadas a las autoridades nacionales competentes ***u otros informes, según proceda;***

(f) el alcance potencial de dicho daño o de dicho impacto adverso, en particular en términos de su intensidad y de su capacidad para afectar a múltiples personas ***o para afectar de manera desproporcionada a un grupo particular de personas***;

(g) la medida en que las personas potencialmente perjudicadas o que sufren un impacto adverso dependen del resultado producido con un sistema de IA, en particular porque por razones prácticas o jurídicas no es razonablemente posible excluirse de dicho resultado;

(h) la medida en que ***existe un desequilibrio de poder, o las personas*** potencialmente perjudicadas o que sufren un impacto adverso se encuentran en una posición vulnerable en relación con quien despliega un sistema de IA, en particular debido a ***su estatus, autoridad***, conocimientos, circunstancias económicas o sociales, o edad;

(i) la medida en que el resultado producido ***por*** un sistema de IA es fácilmente ***corregible o*** reversible, teniendo en ***cuenta las soluciones técnicas disponibles para corregirlo o invertirlo, en*** cuyo caso no se considerarán fácilmente ***corregibles o*** reversibles los resultados que tengan un impacto ***adverso*** en la salud***, la*** seguridad ***o los derechos fundamentales;***

(j) la magnitud y la probabilidad del beneficio del despliegue del sistema de IA para las personas, los grupos o la sociedad en general, incluidas las posibles mejoras en la seguridad de los productos;

(k) en qué medida lo prevé el Derecho de la Unión vigente:

(i) medidas efectivas de reparación en relación con los riesgos que plantea un sistema de IA, con exclusión de las reclamaciones por daños y perjuicios;

(ii) medidas eficaces para prevenir o reducir sustancialmente esos riesgos.

3. La Comisión adoptará actos delegados con arreglo al artículo 97 para modificar la lista del anexo III suprimiendo los sistemas de IA de alto riesgo cuando se cumplan las dos condiciones siguientes:

(a) el sistema de IA de alto riesgo de que se trate ya no plantea riesgos significativos para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

(b) la supresión no disminuye el nivel general de protección de la salud, la seguridad y los derechos fundamentales con arreglo al Derecho de la Unión.

Sección 2

Requisitos de los sistemas de IA de alto riesgo

Artículo 8

Cumplimiento de los requisitos

1. Los sistemas de IA de alto riesgo cumplirán los requisitos establecidos en la presente sección***, teniendo en cuenta sus fines previstos, así como el estado de la técnica generalmente reconocido en materia de IA y tecnologías relacionadas con la IA. El sistema de gestión de riesgos a que se refiere el artículo 9 se tendrá en cuenta a la hora de garantizar el cumplimiento de dichos requisitos***.

2. ***1. Cuando un producto contenga un sistema de IA al que se apliquen los requisitos del presente Reglamento, así como los requisitos de la legislación de armonización de la Unión enumerados en el anexo I, sección A, los proveedores serán responsables de garantizar que su producto cumple plenamente todos los requisitos aplicables exigidos en virtud de la legislación de armonización de la Unión aplicable. 2. Al garantizar la conformidad de los sistemas de IA de alto riesgo a que se refiere el apartado 1 con los requisitos establecidos en la presente sección, y a fin de garantizar la coherencia, evitar duplicaciones y minimizar las cargas adicionales, los proveedores tendrán la opción de integrar, según proceda, los procesos necesarios de ensayo y notificación, la información y la documentación que faciliten en relación con su producto en la documentación y los procedimientos ya existentes y exigidos en virtud de la legislación de armonización de la Unión enumerada en el anexo I, sección A.***

Artículo 9

Sistema de gestión de riesgos

1. Se establecerá, aplicará, documentará y mantendrá un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos se entenderá ***como*** un proceso iterativo continuo, ***planificado y*** ejecutado a lo largo de todo el ciclo de vida de un sistema de IA de alto riesgo, que requiere una ***revisión y*** actualización periódicas y sistemáticas. Comprenderá las siguientes etapas:

(a) la identificación y el análisis de los riesgos conocidos y de los riesgos ***razonablemente*** previsibles ***que el sistema de*** IA de alto riesgo ***puede plantear para la salud, la seguridad o los derechos fundamentales cuando el*** sistema de IA de alto riesgo ***se utiliza de acuerdo con su finalidad prevista;***

(b) la estimación y evaluación de los riesgos que pueden surgir cuando el sistema de IA de alto riesgo se utiliza de acuerdo con su finalidad prevista, y en condiciones de uso indebido razonablemente previsibles;

(c) la evaluación de otros riesgos que puedan surgir, basada en el análisis de los datos recogidos en el sistema de seguimiento poscomercialización contemplado en el artículo 72;

(d) la adopción de medidas de gestión de riesgos ***adecuadas y específicas destinadas a hacer frente a los riesgos identificados con arreglo a la letra a)*** .

3. Los riesgos a que se refiere el ***presente artículo se referirán únicamente a aquellos que puedan mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo, o el suministro de información técnica adecuada.***

4. Las medidas de gestión de riesgos a que se refiere el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible ***interacción*** resultantes de la aplicación combinada de los requisitos establecidos en la presente sección***, con vistas a minimizar los riesgos de forma más eficaz y lograr al mismo tiempo un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos***.

5. Las medidas de gestión de riesgos a que se refiere el apartado 2, letra d), serán tales que el riesgo residual ***pertinente*** asociado a cada peligro, así como el riesgo residual global de los sistemas de IA de alto riesgo, se consideren ***aceptables***.

   A la hora de determinar las medidas de gestión de riesgos más adecuadas, se garantizará lo siguiente:

   (a) eliminación o reducción de los riesgos ***identificados y evaluados con arreglo al apartado 2***, en la medida en que sea ***técnicamente viable,*** mediante un diseño y desarrollo adecuados ***del sistema de IA de alto riesgo;***

   (b) en su caso, aplicación de medidas adecuadas de mitigación y control ***abordar los*** riesgos que no pueden eliminarse;

   (c) el suministro de la información ***exigida*** en virtud del artículo 13 y, en su caso, la formación de ***los encargados del despliegue***. ▌

Con vistas a eliminar o reducir los riesgos relacionados con el uso del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación, la formación que cabe esperar del ***usuario*** y el ***contexto presumible*** en el que se pretende utilizar el sistema.

6. Los sistemas de IA de alto riesgo se someterán a pruebas con el fin de determinar las medidas de gestión de riesgos más adecuadas ***y específicas***. Las pruebas garantizarán que los sistemas de IA de alto riesgo funcionan de manera coherente para los fines previstos y que cumplen los requisitos establecidos en la presente sección.

7. Los procedimientos de ensayo ***podrán incluir ensayos en condiciones reales de conformidad con el artículo 60***.

8. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en cualquier caso, antes de su comercialización o puesta en servicio. Las pruebas se llevarán a cabo en función de parámetros y umbrales probabilísticos ***previamente*** definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo.

9. Al aplicar el sistema de gestión de riesgos previsto en los apartados 1 a 7***, los proveedores tendrán en*** cuenta ***si, habida cuenta de su finalidad prevista,*** el sistema de IA de alto riesgo puede ***repercutir negativamente en los menores de 18 años y, en su caso, en otros grupos de personas vulnerables***.

10. En el caso de los ***proveedores de sistemas de IA de alto riesgo que estén sujetos a requisitos relativos a los procesos internos de gestión de riesgos en virtud de otras disposiciones pertinentes del Derecho de la Unión***, los aspectos previstos en los apartados 1 a 9 ***podrán*** formar parte de los procedimientos de gestión de riesgos establecidos ▌ con arreglo a ***dicho Derecho o combinarse con ellos***.

Artículo 10

Datos y gobernanza de datos

1. Los sistemas de IA de alto riesgo que hagan uso de técnicas que impliquen el entrenamiento de modelos de IA con datos se desarrollarán sobre la base de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad contemplados en los apartados 2 a 5 ***siempre que se utilicen dichos conjuntos de datos***.

2. Los conjuntos de datos de entrenamiento, validación y ensayo estarán sujetos a prácticas de gobernanza y gestión de datos ***adecuadas a la finalidad prevista del sistema de IA de alto riesgo***. Dichas prácticas se referirán en particular a

(a) las opciones de diseño pertinentes;

(b) los procesos de recogida de datos y el origen de los mismos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

▌

(c) operaciones pertinentes de tratamiento de preparación de datos, como anotación, etiquetado, limpieza, ***actualización,*** enriquecimiento y agregación;

(d) la formulación de ▌ supuestos, en particular con respecto a la información que se supone que miden y representan los datos;

(e) ***una*** evaluación de la disponibilidad, cantidad e idoneidad de los conjuntos de datos necesarios;

(f) examen a la vista de posibles sesgos ***que puedan afectar a la salud y la seguridad de las personas, repercutir negativamente en los derechos fundamentales o dar lugar a discriminaciones prohibidas por el Derecho de la Unión, especialmente cuando los resultados de los datos influyan en los insumos para futuras operaciones***;

(g) medidas adecuadas para detectar, prevenir y mitigar los posibles sesgos detectados con arreglo a la letra f);

(h) la identificación de las lagunas o deficiencias de datos ***pertinentes que impidan el cumplimiento del presente Reglamento***, y la forma de subsanar dichas lagunas y deficiencias.

3. ***Los conjuntos de datos*** de entrenamiento, validación y prueba serán pertinentes, ***suficientemente*** representativos ***y, en la medida de lo posible, estarán*** exentos de errores y serán completos a ***la vista de la finalidad prevista***. Tendrán las propiedades estadísticas adecuadas, incluso, en su caso, en lo que se refiere a las personas o grupos de personas en ***relación con los cuales está*** previsto utilizar el sistema de IA de alto riesgo. Estas características de los conjuntos de datos podrán cumplirse a nivel de conjuntos de datos individuales o a nivel de una combinación de los mismos.

4. ***Los conjuntos de datos tendrán*** en cuenta, en la medida en que lo exija la finalidad perseguida, las características o elementos propios del entorno geográfico***, contextual***, conductual o funcional específico en el que esté previsto utilizar el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la detección y corrección de sesgos ▌ en relación con los sistemas de IA de alto riesgo ***de conformidad con el apartado 2, puntos (f) y g) del presente artículo***, los proveedores de dichos sistemas podrán tratar ***excepcionalmente*** categorías especiales de datos personales, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas***. Además de las disposiciones establecidas en el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725, se aplicarán todas las condiciones siguientes para que se produzca dicho tratamiento:***

   (a) la detección y corrección de sesgos no puede realizarse eficazmente mediante el tratamiento de otros datos, incluidos los datos sintéticos o anónimos;

(b) las categorías especiales de datos personales están sujetas a limitaciones técnicas en cuanto a la reutilización de los datos personales, así como a medidas de seguridad y de preservación de la intimidad de última generación, incluida la seudonimización;

(c) las categorías especiales de datos personales estén sujetas a medidas que garanticen que los datos personales tratados estén seguros, protegidos, sujetos a las salvaguardias adecuadas, incluidos controles estrictos y documentación del acceso, para evitar el uso indebido y garantizar que sólo las personas autorizadas con las obligaciones de confidencialidad adecuadas tengan acceso a dichos datos personales;

(d) los datos personales incluidos en las categorías especiales de datos personales no deben ser transmitidos, transferidos o accesibles de otro modo a terceros;

(e) los datos personales de las categorías especiales de datos personales se suprimirán una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, lo que ocurra primero;

(f) los registros de actividades de tratamiento de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680incluyen las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por qué ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

6. ▌Para el desarrollo de sistemas de IA de alto riesgo que ***no utilicen*** técnicas que impliquen el entrenamiento de modelos de IA***, los apartados 2 a 5 se aplican únicamente a los conjuntos de datos de prueba***.

Artículo 11

Documentación técnica

1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de su comercialización o puesta en servicio y se mantendrá actualizada.

   La documentación técnica se elaborará de forma que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en la presente sección y proporcione a las autoridades nacionales competentes y a los organismos notificados la información necesaria de ***forma clara y completa*** para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos establecidos en el anexo IV. Las ***PYME, incluidas las de nueva creación, podrán facilitar los elementos de la documentación técnica especificados en el anexo IV de forma simplificada. A tal efecto, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pequeñas empresas y microempresas. Cuando una PYME, incluida una empresa de nueva creación, opte por facilitar la información requerida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán el formulario a efectos de la evaluación de la conformidad.***

2. 2. Cuando se comercialice o se ponga en servicio un sistema de IA de alto riesgo relacionado con un producto cubierto por la legislación de armonización de la Unión enumerada en la sección A del anexo I, se elaborará un único conjunto de documentación técnica que contenga toda la información establecida en el ***apartado 1,*** así como la información exigida en virtud de dichos actos jurídicos.

3. La Comisión adoptará actos delegados con arreglo al artículo 97 para modificar el anexo IV cuando sea necesario para garantizar que, a la luz del progreso técnico, la documentación técnica proporcione toda la información necesaria para evaluar la conformidad del sistema con los requisitos establecidos en la presente sección.

Artículo 12

Registros

1. Los sistemas de IA de alto riesgo deberán ***permitir técnicamente*** el registro automático de eventos ("logs")

a lo largo de su vida.

2. A ***fin de*** garantizar un nivel de trazabilidad del funcionamiento de un sistema de IA de alto riesgo ▌ adecuado a la finalidad prevista del sistema***, las capacidades de registro permitirán registrar los eventos pertinentes para:***

(a) identificar las situaciones que pueden dar lugar a que el sistema de IA de alto riesgo presente un riesgo en el sentido del apartado 1 del artículo 79 o a una modificación sustancial;

(b) facilitar el seguimiento posterior a la comercialización a que se refiere el artículo 72; y

(c) controlar el funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 26, apartado 6.

▌

3. Para los sistemas de IA de alto riesgo a que se refiere la letra a) del punto 1 del anexo III, las capacidades de registro proporcionarán, como mínimo:

(a) registro del periodo de cada uso del sistema (fecha y hora de inicio y fecha y hora de fin de cada uso);

(b) la base de datos de referencia con la que el sistema ha cotejado los datos de entrada;

(c) los datos de entrada para los que la búsqueda ha dado lugar a una coincidencia;

(d) la identificación de las personas físicas que participan en la verificación de los resultados, según lo dispuesto en el apartado 5 del artículo 14.

Artículo 13

Transparencia y suministro de información a ***los usuarios***

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de forma que se garantice que su funcionamiento es lo suficientemente transparente como para permitir a ***los implantadores*** interpretar los resultados del sistema y utilizarlos adecuadamente. Se garantizará un tipo y un grado de transparencia adecuados ▌ con vistas a lograr el cumplimiento de las obligaciones pertinentes del ***proveedor y del implantador*** establecidas en la sección 3.

2. Los sistemas de IA de alto riesgo irán acompañados de instrucciones de uso en un formato digital adecuado o de otro tipo que incluya información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para quienes los desplieguen.

3. Las ***instrucciones de uso contendrán como mínimo la siguiente información***:

(a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado;

(b) las características, capacidades y limitaciones de rendimiento del sistema de IA de alto riesgo, incluyendo:

(i) su finalidad prevista;

(ii) el nivel de precisión, ***incluidas sus métricas,*** robustez y ciberseguridad a que se refiere el artículo 15, con respecto al cual se ha probado y validado el sistema de IA de alto riesgo y que cabe esperar, así como cualquier circunstancia conocida y previsible que pueda repercutir en ese nivel previsto de precisión, robustez y ciberseguridad;

(iii) cualquier circunstancia conocida o previsible, relacionada con el uso del sistema de IA de alto riesgo de conformidad con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere ***el artículo 9, apartado 2***;

(iv) en su caso, las capacidades y características técnicas del sistema de IA de alto ***riesgo para proporcionar información que sea pertinente para explicar sus resultados;***

(v) ***cuando proceda,*** sus prestaciones ***en relación con las*** personas o grupos de personas específicos en los que se vaya a utilizar el sistema;

(vi) cuando proceda, las especificaciones de los datos de entrada, o cualquier otra información pertinente en cuanto a los conjuntos de datos de entrenamiento, validación y prueba utilizados, teniendo en cuenta la finalidad prevista del sistema de IA de alto riesgo;

(vii) en su caso, información que permita a los responsables de la aplicación interpretar los resultados del sistema de IA de alto riesgo y utilizarlos adecuadamente;

(c) los cambios introducidos en el sistema de IA de alto riesgo y en sus prestaciones que hayan sido determinados previamente por el proveedor en el momento de la evaluación inicial de la conformidad, en su caso;

(d) las medidas de supervisión humana contempladas en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de los sistemas de IA de alto riesgo por parte de ***quienes los despliegan***;

(e) ***los recursos informáticos y de hardware necesarios,*** la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias***, incluida su frecuencia,*** para garantizar el correcto funcionamiento de dicho sistema de IA, incluso en lo que respecta a las actualizaciones de software***;***

(f) en su caso, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita ***a*** los responsables de su despliegue ***recopilar, almacenar e interpretar adecuadamente los registros de conformidad con el artículo 12.***

Artículo 14

Supervisión humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de tal manera, incluso con herramientas adecuadas de interfaz hombre-máquina, que puedan ser supervisados eficazmente por personas físicas durante el periodo en que estén en uso.

2. La supervisión humana tendrá por objeto prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que puedan surgir cuando un sistema de IA de alto riesgo se utilice de acuerdo con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, en particular cuando persistan dichos riesgos a pesar de la aplicación de otros requisitos establecidos en la presente sección.

3. ***Las medidas de*** supervisión ***serán proporcionales a los riesgos, el nivel de autonomía y el contexto de uso del sistema de IA*** de alto riesgo, ***y*** se garantizarán a través de uno de los siguientes ***tipos de*** medidas, o de ambos:

   (a) ***medidas*** identificadas e incorporadas, cuando sea técnicamente viable, al sistema de IA de alto riesgo por el proveedor antes de su comercialización o puesta en servicio;

   (b) ***las medidas*** identificadas por el proveedor antes de comercializar o poner en servicio el sistema de IA de alto riesgo y que conviene que aplique el implantador.

4. ***4. A efectos de la aplicación de los apartados 1, 2 y 3***, ***el sistema de IA de alto riesgo*** se facilitará al usuario de forma ***que se habilite a las personas físicas*** a las que se asigne la supervisión humana, según proceda ***y de forma proporcionada*** a las siguientes circunstancias:

(a) comprender ***adecuadamente las*** capacidades y limitaciones ***pertinentes*** del sistema de IA de alto riesgo y poder supervisar debidamente su funcionamiento, incluso ***con vistas a detectar y abordar*** anomalías, disfunciones y rendimientos inesperados ▌;

(b) ser conscientes de la posible tendencia a confiar automáticamente o a confiar en exceso en los resultados producidos por un sistema de IA de alto riesgo ("sesgo de automatización"), en particular en el caso de los sistemas de IA de alto riesgo utilizados para proporcionar información o recomendaciones para la toma de decisiones por parte de personas físicas;

(c) ▌ interpretar correctamente los resultados del sistema de IA de alto riesgo, teniendo en cuenta, por ***ejemplo,*** las herramientas y métodos de interpretación disponibles;

(d) ▌ decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o hacer caso omiso, anular o invertir de otro modo el resultado del sistema de IA de alto riesgo;

(e) ▌ intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema mediante un botón de ***"parada"*** o un procedimiento similar ***que permita detener el sistema en un estado seguro***.

5. En el caso de los sistemas de IA de alto riesgo a que se refiere la letra a) del punto 1 del Anexo III, las medidas a que se refiere el apartado 3 del presente artículo serán tales que garanticen, además, que el ***responsable del despliegue*** no tome ninguna medida o decisión sobre la base de la identificación resultante del sistema a menos que dicha identificación haya sido verificada y confirmada por ***separado*** por al menos dos personas físicas ***con la competencia, la formación y la autoridad necesarias.***

El requisito de verificación por separado por al menos dos personas físicas no se aplicará a los sistemas de IA de alto riesgo utilizados a efectos policiales, de migración, de control fronterizo o de asilo, cuando el Derecho de la Unión o nacional considere desproporcionada la aplicación de este requisito.

Artículo 15

Precisión, solidez y ciberseguridad

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de manera que alcancen un nivel adecuado de precisión, solidez y ciberseguridad, y que funcionen de manera coherente en esos aspectos a lo largo de su ciclo de vida.

2. ***Para abordar los aspectos técnicos de cómo medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 y cualquier otra métrica de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y las organizaciones pertinentes, como las autoridades de metrología y evaluación comparativa, fomentará, según proceda, el desarrollo de parámetros de referencia y metodologías de medición.***

3. Los niveles de precisión y las métricas de precisión pertinentes de los sistemas de IA de alto riesgo se declararán en las instrucciones de uso adjuntas.

4. Los sistemas de IA de alto riesgo serán ***lo*** más resistentes posible ***frente a*** los errores, fallos o incoherencias que puedan producirse en el sistema o en el entorno en el que opera el sistema, en particular debido a su interacción con personas físicas u otros sistemas. ***Se adoptarán medidas técnicas y organizativas a este respecto.***

   La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones técnicas de redundancia, que pueden incluir planes de respaldo o a prueba de fallos.

   Los sistemas de IA de alto riesgo que sigan aprendiendo después de su comercialización o puesta en servicio se desarrollarán de forma que ***se elimine o reduzca en la medida de lo posible el riesgo de que los resultados posiblemente sesgados influyan en*** los datos de entrada para futuras operaciones ("bucles de retroalimentación"), y de forma que se garantice que cualquier bucle de retroalimentación de este tipo se aborde debidamente con medidas de mitigación adecuadas.

5. Los sistemas de IA de alto riesgo deberán ser resistentes a los intentos de terceros no autorizados de alterar su uso***, resultados*** o rendimiento aprovechando las vulnerabilidades del sistema.

Las soluciones técnicas destinadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo deberán ser adecuadas a las circunstancias pertinentes y a los riesgos.

Las soluciones técnicas para abordar las vulnerabilidades específicas de la IA incluirán, cuando proceda, medidas para prevenir***, detectar, responder, resolver*** y controlar los ataques que intenten manipular el conjunto de datos de entrenamiento ("envenenamiento de datos"), ***o los componentes preentrenados utilizados en el entrenamiento ("envenenamiento del modelo"),*** las entradas diseñadas para provocar que el modelo de IA cometa un error ("ejemplos adversos" ***o "evasión del modelo"***), los ***ataques a la confidencialidad*** o los defectos del modelo.

Sección 3

Obligaciones de los proveedores e *implantadores* de sistemas de IA de alto riesgo y otras partes

Artículo 16

Obligaciones de los proveedores de sistemas de IA de alto riesgo

Los proveedores de sistemas de IA de alto riesgo deberán:

(a) garantizar que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos en la sección 2;

(b) indicar en el sistema de IA de alto riesgo o, cuando ello no sea posible, en su envase o en la documentación que lo acompañe, según proceda, su nombre, nombre comercial registrado o marca comercial registrada, la dirección en la que se les puede contactar;

(c) disponer de un sistema de gestión de la calidad que se ajuste a lo dispuesto en el artículo 17;

(d) ***conservar la*** documentación ***mencionada en el artículo 18***;

(e) cuando estén bajo su control, conservar los registros generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere ***el artículo 19***;

(f) garantizar que el sistema de IA de alto riesgo se somete al correspondiente procedimiento de evaluación de la conformidad ***a que se refiere el artículo 43***, antes de su comercialización o puesta en servicio;

(g) elaborar una declaración UE de conformidad con arreglo al artículo 47;

(h) colocar el marcado CE en el sistema de IA de alto riesgo o, cuando ello no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar su conformidad con el presente Reglamento, de conformidad con el artículo 48;

(i) cumplir las obligaciones de registro contempladas en el ***apartado 1 del*** artículo 49;

(j) adoptar las medidas correctoras necesarias ***y facilitar la información exigida en el artículo 20***;

(k) ***previa*** solicitud ***motivada*** de una autoridad nacional competente, demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2;

(l) garantizar que el sistema de IA de alto riesgo cumple los requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

Artículo 17

Sistema de gestión de la calidad

1. Los proveedores de sistemas de IA de alto riesgo implantarán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema estará documentado de forma sistemática y ordenada en forma de políticas, procedimientos e instrucciones escritas, e incluirá al menos los siguientes aspectos:

   (a) una estrategia de cumplimiento de la normativa, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y los procedimientos de gestión de las modificaciones del sistema de IA de alto riesgo;

   (b) técnicas, procedimientos y acciones sistemáticas que deben utilizarse para el diseño, el control del diseño y la verificación del diseño del sistema de IA de alto riesgo;

   (c) técnicas, procedimientos y acciones sistemáticas que se utilizarán para el desarrollo, el control de calidad y la garantía de calidad del sistema de IA de alto riesgo;

   (d) los procedimientos de examen, prueba y validación que deben llevarse a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, y la frecuencia con que deben realizarse;

(e) las especificaciones técnicas, incluidas las normas, que deben aplicarse y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad ***o no cubran todos los requisitos pertinentes establecidos en la sección 2,*** los medios que deben utilizarse para garantizar que el sistema de IA de alto riesgo cumple ***dichos*** requisitos ▌ ;

(f) los sistemas y procedimientos de gestión de datos, incluida la ***adquisición*** de datos***,*** ***la*** recogida de ***datos***, el análisis de datos, el etiquetado de datos, el almacenamiento de datos, el filtrado de datos, la extracción de datos, la agregación de datos, la conservación de datos y cualquier otra operación relativa a los datos que se realice antes y a efectos de la comercialización o la puesta en servicio de sistemas de IA de alto riesgo;

(g) el sistema de gestión de riesgos a que se refiere el artículo 9;

(h) la creación, aplicación y mantenimiento de un sistema de seguimiento postcomercialización, de conformidad con el artículo 72;

(i) los procedimientos relacionados con la notificación de ***un incidente grave*** de conformidad con el artículo 73;

(j) la gestión de la comunicación con las autoridades nacionales competentes, ***otras*** autoridades ***pertinentes,*** incluidas ***las que*** facilitan o apoyan el acceso a los datos, organismos notificados, otros operadores, clientes u otras partes interesadas;

(k) sistemas y procedimientos de registro de toda la documentación e información pertinentes;

(l) gestión de los recursos, incluidas las medidas relacionadas con la seguridad del abastecimiento;

(m) un marco de rendición de cuentas que establezca las responsabilidades de la dirección y del resto del personal en relación con todos los aspectos enumerados en este apartado.

2. La aplicación de los aspectos contemplados en el apartado 1 será proporcional al tamaño de la organización del proveedor. ***En cualquier caso, los proveedores deberán respetar el grado de rigor y el nivel de protección necesarios para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.***

3. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o a una función equivalente en virtud de la legislación sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicha legislación.

4. Para los proveedores que sean entidades financieras ***sujetas a requisitos relativos a su*** gobernanza***, disposiciones o procesos*** internos con ***arreglo a la legislación de la Unión en materia de servicios financieros***, la obligación de ***establecer*** un sistema de gestión de la calidad, ***con excepción del apartado 1, letras g), h) e i),*** del presente artículo, se considerará cumplida mediante el cumplimiento de las normas sobre disposiciones ***o procesos de*** gobernanza interna con arreglo a ***la legislación de la Unión en materia de servicios financieros pertinente***. A tal efecto, se tendrán en cuenta las normas armonizadas a que se refiere el artículo 40.

Artículo 18

Conservación de la documentación

1. ***El proveedor mantendrá a disposición de las autoridades nacionales competentes, durante un período que finalizará diez años después de la comercialización o puesta en servicio del sistema de IA de alto riesgo:***

   (a) la documentación técnica contemplada en el artículo 11;

   (b) la documentación relativa al sistema de gestión de la calidad a que se refiere el artículo 17;

   (c) la documentación relativa a las modificaciones aprobadas por los organismos notificados, en su caso;

   (d) las decisiones y otros documentos emitidos por los organismos notificados, en su caso;

   (e) la declaración UE de conformidad a que se refiere el artículo 47.

2. ***Cada Estado miembro determinará las condiciones en las que la documentación contemplada en el apartado 1 permanecerá a disposición de las autoridades nacionales competentes durante el período indicado en dicho apartado para los casos en que un prestador o su representante autorizado establecido en su territorio quiebre o cese su actividad antes del final de dicho período.***

3. Los proveedores que sean entidades financieras sujetas ***a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación de la Unión en materia de servicios financieros*** conservarán la documentación técnica como parte de la documentación ***conservada en virtud de la legislación de la Unión en materia de servicios financieros pertinente***.

I

Artículo 19 Registros generados automáticamente

1. Los proveedores de sistemas de IA de alto riesgo conservarán los registros a que se refiere ***el artículo 12, apartado 1,*** generados automáticamente por sus sistemas de IA de alto riesgo, en la medida en que dichos registros estén bajo su control***. Sin perjuicio del Derecho de la*** Unión o nacional aplicable, los registros se conservarán durante un período ▌ adecuado ***a*** la finalidad prevista del sistema de IA de alto ***riesgo, de al menos seis meses, salvo disposición en contrario del*** Derecho de la Unión o nacional ***aplicable, en particular del Derecho de la Unión en materia de protección de datos personales***.

2. Los proveedores que sean entidades financieras ***sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos con arreglo a la legislación de la Unión en materia de servicios financieros*** conservarán los registros generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación ***conservada*** con arreglo a ***la legislación pertinente en materia de servicios financieros***.

Artículo 20

Acciones correctoras ***y deber de información***

1. 1. Los proveedores de sistemas de IA de alto riesgo que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han introducido en el mercado o puesto en servicio no es conforme con el presente Reglamento adoptarán inmediatamente las medidas correctoras necesarias para hacerlo conforme, retirarlo del mercado***,*** ***inutilizarlo*** o recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo en cuestión y, en su caso, a los ***responsables del despliegue, al*** representante autorizado y a los importadores.

2. ***Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, investigará inmediatamente las causas, en colaboración con el implantador notificante, en su caso, e informará a las autoridades de vigilancia del mercado del Estado miembro o de los Estados miembros en los que comercializaron el sistema de IA de alto riesgo y, en su caso, al organismo notificado que expidió un certificado para dicho sistema de IA de alto riesgo de conformidad con el artículo 44, en particular, de la naturaleza del incumplimiento y de las medidas correctoras pertinentes adoptadas.***

Artículo 21

Cooperación con las autoridades competentes

1. Los proveedores de sistemas de IA de alto riesgo, previa solicitud ***motivada*** de una ▌ autoridad competente, facilitarán a dicha autoridad ▌ toda la información y documentación necesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, en ***una lengua fácilmente comprensible*** para la ***autoridad en una de las lenguas oficiales de las instituciones de la Unión indicada por el Estado miembro de que se trate***.

2. ***Previa solicitud motivada de una autoridad nacional competente, los proveedores también darán a la autoridad nacional competente solicitante, según proceda, acceso a los registros generados automáticamente por el sistema de IA de alto riesgo a que se refiere el artículo 12, apartado 1, en la medida en que dichos registros estén bajo su control.***

3. Toda información obtenida por una autoridad nacional competente en virtud del presente artículo se tratará respetando las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 22

Representantes autorizados de los proveedores de sistemas de IA de alto riesgo

1. Antes de comercializar sus sistemas de IA de alto riesgo en el mercado de la Unión, los proveedores ▌ establecidos en terceros países designarán, mediante mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. El prestador permitirá a su representante autorizado realizar las tareas especificadas en el mandato recibido del prestador.

3. El representante autorizado realizará las tareas especificadas en el mandato recibido del proveedor. ***Facilitará una copia del mandato a las autoridades de vigilancia del mercado que lo soliciten, en una de las lenguas oficiales de las instituciones de la Unión, según lo indicado por la autoridad nacional competente. A efectos del presente Reglamento,*** el mandato facultará al representante autorizado para llevar a cabo las siguientes tareas:

(a) comprobar que se han elaborado la declaración UE de conformidad y la documentación técnica a que se refiere el artículo 11 y que el proveedor ha llevado a cabo un procedimiento adecuado de evaluación de la conformidad;

(b) mantener ***a disposición*** de las ***autoridades nacionales competentes y de las autoridades u organismos nacionales a que se refiere el artículo 74, apartado 10, durante un período de diez años a partir de la comercialización o puesta en servicio del sistema de IA de alto riesgo, los datos de contacto*** del ***proveedor que haya designado al representante autorizado, una copia de la declaración UE de conformidad, la documentación técnica y, si procede, el certificado expedido por el organismo notificado***;

(c) facilitar a una autoridad nacional competente, previa solicitud motivada, toda la información y documentación***, incluida la mencionada en la letra b) del presente párrafo,*** necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, incluido el acceso a los registros***, a que se refiere el artículo 12, apartado 1,*** generados automáticamente por el sistema de IA de alto riesgo, en la medida en que dichos registros estén bajo el control del proveedor ▌;

(d) cooperar con las autoridades competentes ▌, previa solicitud motivada, en cualquier acción que éstas emprendan en relación con el ***sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que plantea el sistema de IA de alto riesgo;***

(e) en su caso, cumplir las obligaciones de registro a que se refiere el apartado 1 del artículo 49 o, si el registro lo efectúa el propio prestador, garantizar que la información a que se refiere la sección A del ***anexo VIII es correcta.***

El mandato facultará al representante autorizado para que las autoridades competentes se dirijan a él, además de al prestador o en su lugar, para todas las cuestiones relacionadas con el cumplimiento del presente Reglamento.

4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor actúa de forma contraria a las obligaciones que le incumben en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la autoridad de vigilancia del mercado del Estado miembro en el que esté situado o establecido, así como, en su caso, al organismo notificado pertinente, de la terminación del mandato y de los motivos de la misma.

Artículo 23

Obligaciones de los importadores

1. Antes de comercializar un sistema de IA de alto riesgo, los importadores se asegurarán de que ***el sistema es conforme con el presente Reglamento verificando que***:

(a) el proveedor del sistema de IA de alto riesgo haya llevado a cabo el ***correspondiente*** procedimiento de evaluación de la conformidad ***a que se refiere el artículo 43;***

(b) el proveedor haya elaborado la documentación técnica de conformidad con ***el artículo 11 y el*** anexo IV;

(c) el sistema lleva el marcado ***CE*** requerido y va acompañado de la ***declaración de conformidad de la UE*** y de las instrucciones de uso***;***

(d) el prestador haya designado a un representante autorizado de conformidad con el apartado 1 del artículo 22.

2. Cuando un importador ***tenga*** motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, ***o está falsificado, o va acompañado de documentación falsificada,*** no introducirá dicho sistema en el mercado hasta que sea conforme. Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, el importador informará de ello al proveedor del sistema***, a los representantes autorizados*** y a las autoridades de vigilancia del mercado.

3. Los importadores indicarán su nombre, su nombre comercial registrado o marca comercial registrada y la dirección en la que se les puede contactar en relación con el sistema de IA de alto riesgo en su embalaje o en la documentación que lo acompañe, ***cuando*** proceda.

4. 1. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que las condiciones de almacenamiento o transporte, en su caso, no comprometen el cumplimiento de los requisitos establecidos en la sección 2.

5. ***Los importadores conservarán, durante un período de diez años después de la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad.***

6. Los importadores facilitarán a las autoridades nacionales competentes, previa solicitud motivada, toda ***la*** información y documentación necesarias, ***incluida la conservada con arreglo al apartado 5,*** para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua fácilmente comprensible para ***ellas. A tal fin, velarán asimismo por que la documentación técnica pueda ponerse a disposición de dichas autoridades***.

7. ***Los importadores cooperarán con las autoridades nacionales competentes en cualquier acción que éstas emprendan en relación con un sistema de IA de alto riesgo que los importadores hayan comercializado, en particular para reducir y mitigar los riesgos que plantee.***

Artículo 24

Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores comprobarán que lleva el marcado CE requerido, que va acompañado de ***una copia de la declaración UE de conformidad*** y de las instrucciones de uso, y que el proveedor y el importador del sistema, según proceda, han cumplido ***sus*** respectivas obligaciones establecidas en ***el artículo 16, letras b) y c), y en el artículo 23, apartado 3***.

2. Cuando un distribuidor considere o tenga motivos para considerar***, sobre la base de la información que obra en su poder, que un sistema de IA de alto riesgo*** no es conforme con los requisitos establecidos en la sección 2, no comercializará el sistema de IA de alto riesgo hasta que el sistema sea conforme con dichos requisitos. Además, cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, el distribuidor informará de ello al proveedor o al importador del sistema, según proceda.

3. 1. Mientras sean responsables de un sistema de IA de alto riesgo, los distribuidores se asegurarán de que, en su caso, las condiciones de almacenamiento o transporte no comprometan la conformidad del sistema con los requisitos establecidos en la sección 2.

4. El distribuidor que considere o tenga motivos para considerar***, sobre la base de la información que obra en su poder,*** que un sistema de IA de alto riesgo que ha comercializado no es conforme con los requisitos establecidos en la sección 2, adoptará las medidas correctoras necesarias para que el sistema sea conforme con dichos requisitos, retirarlo del mercado o recuperarlo, o se asegurará de que el proveedor, el importador o cualquier operador pertinente, según proceda, adopte esas medidas correctoras. Cuando el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, el distribuidor informará inmediatamente de ello al proveedor ***o importador del sistema y a las*** autoridades nacionales competentes de los Estados miembros en los que haya comercializado el producto, facilitando detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad nacional competente, los distribuidores de ***un sistema de IA de alto riesgo*** facilitarán a dicha autoridad toda la información y documentación ***relativas a sus actuaciones con arreglo a los apartados 1 a 4*** necesarias para demostrar la conformidad de dicho sistema con los requisitos establecidos en la sección 2. ▌

6. Los distribuidores cooperarán con las autoridades nacionales competentes en cualquier acción que éstas emprendan en relación con un sistema de IA de alto riesgo que hayan comercializado, en particular para reducir o mitigar el riesgo que plantea.

Artículo 25

Responsabilidades a lo largo de la cadena de valor de la IA

1. Cualquier distribuidor, importador, ***implantador*** u otro tercero se considerará proveedor de ***un sistema de IA de alto*** riesgo a efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor con arreglo al artículo 16, en cualquiera de las siguientes circunstancias:

(a) ***ponen su nombre o marca comercial en un sistema de IA de alto*** riesgo ***ya*** comercializado o puesto en servicio***, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones correspondientes se asignen de otro modo;***

(b) ***introducen una modificación sustancial en*** un sistema de ***IA de alto riesgo que*** ya ha ***sido*** comercializado o que ***ya ha sido*** puesto en servicio de tal forma ***que sigue siendo un sistema de IA de alto riesgo con arreglo al artículo 6***;

(c) modifiquen la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido clasificado como de alto riesgo y que ya haya sido comercializado o puesto en servicio, de tal forma que el sistema de IA en cuestión se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

▌

2. Cuando se den las circunstancias a que se refiere el apartado 1, el proveedor que inicialmente comercializó o puso en servicio el sistema de IA ▌ dejará de ser considerado proveedor ***de ese sistema de IA específico*** a efectos del presente Reglamento. ***Dicho proveedor inicial cooperará estrechamente con los nuevos proveedores y pondrá a su disposición la información necesaria y facilitará el acceso técnico y demás asistencia que razonablemente quepa esperar y que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. El presente apartado no se aplicará en los casos en que el proveedor inicial haya especificado claramente que su sistema de IA no se va a transformar en un sistema de IA de alto riesgo y, por lo tanto, no esté sujeto a la obligación de entregar la documentación.***

3. ***En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos*** cubiertos por la legislación de armonización de la Unión ***enumerada en la sección A del anexo I, se considerará que el fabricante del producto es el proveedor del sistema de IA de alto riesgo, y estará sujeto a las obligaciones previstas en el artículo 16 en cualquiera de las siguientes circunstancias:***

(a) el sistema de IA de alto riesgo se comercializa junto con el producto bajo el nombre o la marca del fabricante del producto;

(b) el sistema de IA de alto riesgo se pone en servicio con el nombre o la marca del fabricante del producto después de que éste se haya comercializado.

4. ***El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo por escrito, la información, las capacidades, el acceso técnico y demás asistencia necesarios basados en el estado de la técnica generalmente reconocido, a fin de que el proveedor del sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. El presente apartado no se aplicará a los terceros que pongan a disposición del público herramientas, servicios, procesos o componentes, distintos de los modelos de IA de uso general, con arreglo a una licencia libre y abierta.***

La Oficina de AI podrá elaborar y recomendar cláusulas modelo voluntarias para los contratos entre proveedores de sistemas de AI de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen para sistemas de AI de alto riesgo o se integren en ellos. Al elaborar dichas cláusulas modelo voluntarias, la Oficina de IA tendrá en cuenta los posibles requisitos contractuales aplicables en sectores o casos empresariales específicos. Las cláusulas tipo voluntarias se publicarán y estarán disponibles gratuitamente en un formato electrónico de fácil utilización.

5. ***Los apartados 2 y 3 se entienden sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual, la información comercial confidencial y los secretos comerciales de conformidad con el Derecho de la Unión y nacional.***

Artículo 26

Obligaciones de los ***implantadores*** *de sistemas de IA de alto riesgo*

1. ***Los responsables del despliegue*** de sistemas de IA de alto riesgo ***adoptarán las medidas técnicas y organizativas adecuadas para garantizar que*** utilizan dichos sistemas de conformidad con las instrucciones de uso que acompañan a los sistemas, con arreglo a los apartados 3 y 6.

2. ***Los responsables del despliegue asignarán la supervisión humana a personas físicas que tengan la competencia, formación y autoridad necesarias, así como el apoyo necesario.***

.

3. Las obligaciones establecidas en los apartados 1 ***y 2*** se entienden sin perjuicio de otras obligaciones ***del responsable del despliegue*** en virtud del Derecho de la Unión o nacional y de la libertad del ***responsable del despliegue*** de organizar sus propios recursos y actividades con el fin de aplicar las medidas de supervisión humana indicadas por el proveedor.

4. Sin perjuicio de lo dispuesto en los apartados 1 ***y 2***, en la medida en que el ***implantador*** ejerza control sobre los datos de entrada, garantizará que dichos datos sean pertinentes ***y suficientemente representativos a*** la vista de la finalidad prevista del sistema de IA de alto riesgo.

5. ***Los responsables del despliegue*** supervisarán el funcionamiento del sistema de IA de alto riesgo sobre la base de las instrucciones de uso ***y, en su caso, informarán a los proveedores de conformidad con el artículo 72***. Cuando los responsables del despliegue tengan motivos para considerar que el uso del sistema de IA de alto riesgo de conformidad con las instrucciones puede presentar un riesgo en el sentido del artículo 79, apartado 1, informarán ***sin demora injustificada*** al proveedor o distribuidor y a la ***autoridad de vigilancia del mercado pertinente, y*** suspenderán el uso de dicho sistema. Cuando los responsables del despliegue hayan detectado un incidente grave, también informarán ***inmediatamente*** de dicho incidente ***primero*** al proveedor ***y después al importador*** o distribuidor ***y a las autoridades de vigilancia del mercado pertinentes***. ***Si el responsable del despliegue no puede ponerse en contacto con el proveedor, se aplicará el artículo 73 mutatis mutandis. Esta obligación no cubrirá los datos operativos sensibles de los implantadores de sistemas de IA que sean autoridades policiales***.

   En el caso de ***los implementadores*** que sean entidades financieras ***sujetas a requisitos relativos a su*** gobernanza***, disposiciones o procesos internos con arreglo a la legislación de la Unión en materia de servicios financieros***, la obligación de supervisión establecida en el párrafo primero se considerará cumplida mediante el cumplimiento de las normas sobre disposiciones, procesos y mecanismos de gobernanza interna con arreglo a ***la legislación pertinente en materia de servicios financieros***.

6. ***Los implantadores*** de sistemas de IA de alto riesgo conservarán los registros generados automáticamente por dicho sistema de IA de alto riesgo ▌ en la medida en que dichos registros estén bajo su control, ▌ durante un período ▌ adecuado ***a*** la finalidad prevista del sistema de IA de alto riesgo***, de al menos seis meses, salvo disposición en contrario*** del Derecho de la Unión o nacional ***aplicable, en particular del Derecho de la Unión en materia de protección de datos personales***.

Los Desplegadores que sean entidades financieras ***sujetas a requisitos relativos a su gobernanza, disposiciones o procesos internos en virtud de la legislación sobre servicios financieros de la Unión*** mantendrán los registros como parte de la documentación ***conservada*** de conformidad con la ***legislación pertinente sobre servicios financieros de la Unión***.

7. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empresarios informarán a los representantes de los trabajadores y a los trabajadores afectados de que van a estar sometidos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, en su caso, de conformidad con las normas y procedimientos establecidos en el Derecho y las prácticas de la Unión y nacionales en materia de información a los trabajadores y a sus representantes.

8. Los implantadores de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos u organismos de la Unión cumplirán las obligaciones de registro a que se refiere el artículo 49. Cuando dichos implantadores descubran que el sistema de IA de alto riesgo que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 71, no utilizarán dicho sistema e informarán de ello al proveedor o al distribuidor.

9. ***Cuando proceda, los responsables del despliegue*** de sistemas de IA de alto riesgo utilizarán la información facilitada en virtud del artículo 13 del presente Reglamento para cumplir con su obligación de realizar una evaluación de impacto relativa a la protección de datos con arreglo al artículo 35 del Reglamento (UE) 2016/679 o al artículo 27 de la Directiva (UE) 2016/680. ▌

10. ***Sin perjuicio de lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación para el registro selectivo de una persona sospechosa o condenada por haber cometido una infracción penal, el implantador de un sistema de IA*** de alto riesgo ***para la identificación biométrica a distancia solicitará una autorización, ex ante, o sin demora indebida y en un plazo máximo de 48 horas, por una autoridad judicial o una autoridad administrativa cuya decisión sea vinculante y susceptible de control jurisdiccional, para la utilización de dicho sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso basada en hechos objetivos y verificables directamente relacionados con el delito. Cada uso se limitará a lo estrictamente necesario para la investigación de una infracción penal específica.***

Si se deniega la autorización solicitada prevista en el párrafo primero, se interrumpirá con efecto inmediato el uso del sistema de identificación biométrica a distancia vinculado a dicha autorización solicitada y se suprimirán los datos personales vinculados al uso del sistema de IA de alto ***riesgo para el que se solicitó la autorización.***

En ningún caso se utilizará este sistema de IA de alto riesgo ***para la identificación biométrica a distancia con fines policiales de forma no selectiva, sin relación alguna con un delito, un procedimiento penal, una amenaza real y actual o real y previsible de delito, o la búsqueda de una persona desaparecida concreta. Se garantizará que las autoridades policiales no puedan tomar ninguna decisión que produzca un efecto jurídico adverso sobre una persona basándose únicamente en los resultados de dichos sistemas de identificación biométrica a distancia.***

El presente apartado se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 y en el artículo 10 de la Directiva (UE) 2016/680 para el tratamiento de datos biométricos.

Independientemente de la finalidad o de quien lo despliegue, cada uso de estos sistemas de IA de alto riesgo ***se documentará en el expediente policial pertinente y se pondrá a disposición de la autoridad de vigilancia del mercado pertinente y de la autoridad nacional de protección de datos previa solicitud, excluida la divulgación de datos operativos sensibles relacionados con la aplicación de la ley. El presente párrafo se entenderá sin perjuicio de las facultades conferidas por***
Directiva (UE) 2016/680 sobre las autoridades de supervisión.

Los responsables del despliegue presentarán informes anuales a las autoridades nacionales competentes de vigilancia del mercado y de protección de datos sobre el uso que hacen de los sistemas de identificación biométrica a distancia, excluyendo la divulgación de datos operativos sensibles relacionados con la aplicación de la ley. Los informes podrán agregarse para cubrir más de un despliegue.

Los Estados miembros podrán introducir, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica a distancia.

11. Sin perjuicio de lo dispuesto en el artículo 50 del presente Reglamento, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán a las personas físicas de que están sujetas al uso del sistema de IA de alto riesgo. Para los sistemas de IA de alto riesgo utilizados con fines policiales se aplicará el artículo 13 de la Directiva (UE) 2016/680.

12. Los responsables del despliegue cooperarán con las autoridades nacionales competentes en cualquier acción que éstas emprendan en relación con el sistema de IA de alto riesgo con el fin de aplicar el presente Reglamento.

Artículo 27

Evaluación del impacto sobre los derechos fundamentales de los sistemas de IA de alto riesgo

1. ***Antes de proceder al despliegue de un sistema de IA de alto riesgo contemplado en el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público o entidades privadas que presten servicios públicos, y los responsables del despliegue de sistemas de IA de alto riesgo contemplados en el*** anexo III***, punto 5, letras b)*** y c)***, llevarán a cabo una evaluación del impacto sobre los derechos fundamentales que el uso de dicho sistema pueda producir. A tal efecto, los implantadores realizarán una evaluación consistente en:***

(a) ***una descripción de los procesos del implantador en los que se utilizará el sistema de IA de alto riesgo de acuerdo con su finalidad prevista;***

(b) ***una descripción del período de tiempo y la frecuencia con que se prevé utilizar cada sistema de IA de alto riesgo;***

(c) ***las categorías de personas físicas y grupos que puedan verse afectados por su uso en el contexto específico;***

(d) los riesgos específicos de daños que puedan afectar a las categorías de personas o grupos de personas identificados con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el prestador con arreglo al artículo 13;

(e) una descripción de la aplicación de las medidas de supervisión humana, de acuerdo con las instrucciones de uso;

(f) las medidas que deben adoptarse en caso de que se materialicen esos riesgos, incluidas las disposiciones relativas a la gobernanza interna y los mecanismos de denuncia.

2. La obligación establecida en el apartado 1 se aplica al primer uso del sistema de IA de alto riesgo. El implantador podrá, en casos similares, basarse en las evaluaciones de impacto sobre los derechos fundamentales realizadas anteriormente o en las evaluaciones de impacto existentes llevadas a cabo por el proveedor. Si, durante la utilización del sistema de IA de alto riesgo, el implantador considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ya no está actualizado, tomará las medidas necesarias para actualizar la información.

3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, incluyendo la cumplimentación y presentación de la plantilla a que se refiere el apartado 5 del presente artículo como parte de la notificación. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de dicha obligación de notificación.

4. ***Si alguna de las obligaciones establecidas en el presente artículo ya se cumple como resultado de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos.***

5. ***La Oficina de AI elaborará un modelo de cuestionario, incluso mediante una herramienta automatizada, para facilitar a los responsables del despliegue el cumplimiento de sus obligaciones en virtud del presente artículo de forma simplificada.***

Sección 4

Autoridades notificantes y organismos notificados

Artículo 28

Autoridades de notificación

1. 1. Cada Estado miembro designará o establecerá ***al menos una*** autoridad notificante responsable de establecer y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad y de su supervisión. ***Estos procedimientos se desarrollarán en cooperación con las autoridades notificantes de todos los Estados miembros.***

2. Los Estados miembros podrán ***decidir que la evaluación y el seguimiento a que se refiere el apartado 1 sean realizados por*** un organismo nacional de acreditación ***en el sentido del*** Reglamento (CE) nº 765/2008 ▌ ***y de conformidad con el mismo***.

3. Las autoridades notificantes se establecerán, organizarán y gestionarán de manera que no exista ningún conflicto de intereses con los organismos de evaluación de la conformidad y se preserve la objetividad e imparcialidad de sus actividades.

4. Las autoridades notificantes se organizarán de forma que las decisiones relativas a la notificación de los organismos de evaluación de la conformidad sean adoptadas por personas competentes distintas de las que llevaron a cabo la evaluación de dichos organismos.

5. Las autoridades notificantes no ofrecerán ni ejercerán ninguna actividad que efectúen los organismos de evaluación de la conformidad, ni servicios de consultoría en condiciones comerciales o de competencia.

6. Las autoridades notificantes salvaguardarán la confidencialidad de la información que obtengan, de conformidad ***con el artículo 78***.

7. Las autoridades notificantes dispondrán de un número ***adecuado de*** personal competente para el correcto desempeño de sus funciones. El ***personal competente poseerá los conocimientos especializados necesarios, en su caso, para el desempeño de su función, en ámbitos como las tecnologías de la información, la inteligencia artificial y el Derecho, incluida la supervisión de los derechos fundamentales.***

Artículo 29

Solicitud de notificación de un organismo de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación a la autoridad notificante del Estado miembro en el que estén establecidos.

2. La solicitud de notificación irá acompañada de una descripción de las actividades de evaluación de la conformidad, del módulo o módulos de evaluación de la conformidad y de los ***tipos de sistemas de IA*** para los que el organismo de evaluación de la conformidad se considere competente, así como de un certificado de acreditación, si lo hay, expedido por un organismo nacional de acreditación, que declare que el organismo de evaluación de la conformidad cumple los requisitos establecidos en el artículo 31.

   Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante con arreglo a cualquier otra legislación de armonización de la Unión.

3. Cuando el organismo de evaluación de la conformidad en cuestión no pueda facilitar un certificado de acreditación, entregará a la autoridad notificante ***todas las*** pruebas documentales necesarias para la verificación, el reconocimiento y el seguimiento regular del cumplimiento de los requisitos establecidos en el artículo 31.

4. En el caso de los organismos notificados designados con arreglo a cualquier otra legislación de armonización de la Unión, todos los documentos y certificados relacionados con dichas designaciones podrán utilizarse para apoyar su procedimiento de designación con arreglo al presente Reglamento, según proceda. ***El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 del presente artículo siempre que se produzcan cambios pertinentes, a fin de que la autoridad responsable de los organismos notificados pueda supervisar y verificar el cumplimiento permanente de todos los requisitos establecidos en el artículo 31.***

Artículo 30

Procedimiento de notificación

1. Las autoridades notificantes solo podrán ***notificar*** organismos de evaluación de la conformidad que satisfagan los requisitos establecidos en el artículo 31.

2. 2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, por medio de la herramienta de notificación electrónica desarrollada y gestionada por la Comisión, ***cada organismo de evaluación de la conformidad a que se refiere el apartado 1***.

3. 3. La notificación a que se refiere el ***apartado 2 del presente artículo*** incluirá información pormenorizada de las actividades de evaluación de la conformidad, el módulo o los módulos de evaluación de la conformidad, los ***tipos de sistemas de IA*** de que se trate ***y la correspondiente certificación de competencia. 4. Cuando una notificación no se base en un certificado de acreditación como el mencionado en el apartado 2 del artículo 29, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones adoptadas para garantizar que se supervisará periódicamente a dicho organismo y que este seguirá cumpliendo los requisitos establecidos en el artículo 31***.

4. El organismo de evaluación de la conformidad en cuestión sólo podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no han formulado ninguna objeción en el plazo de ***dos semanas a partir de la notificación por parte de una autoridad notificante, cuando ésta incluya un certificado de acreditación con arreglo al apartado 2 del artículo 29, o de dos meses*** a partir de la notificación ***por parte de la autoridad notificante, cuando ésta incluya las pruebas documentales con arreglo al apartado 3 del artículo 29***.

5. ***En caso de que se planteen objeciones, la Comisión consultará sin demora a los Estados miembros pertinentes y al organismo de evaluación de la conformidad. A la vista de las mismas, la Comisión decidirá si la autorización está justificada. La Comisión comunicará su decisión al Estado miembro interesado y al organismo de evaluación de la conformidad pertinente.***

Artículo 31

Requisitos relativos a los organismos notificados

1. Los ***organismos*** notificados ***se crearán con arreglo a la legislación nacional de un Estado miembro y tendrán personalidad jurídica***.

2. Los organismos notificados deberán cumplir los requisitos de organización, gestión de la calidad, recursos y procesos necesarios para el desempeño de sus funciones, ***así como los requisitos de ciberseguridad adecuados***.

3. La estructura organizativa, la asignación de responsabilidades, las líneas jerárquicas y el funcionamiento de los organismos notificados garantizarán la confianza en su rendimiento y en los resultados de las actividades de evaluación de la conformidad que realizan los organismos notificados.

4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual realicen actividades de evaluación de la conformidad. Los organismos notificados también serán independientes de cualquier otro agente que tenga un interés económico en los sistemas de IA de alto riesgo evaluados, así como de cualquier competidor del proveedor. ***Esto no impedirá el uso de los sistemas de IA de alto riesgo evaluados que sean necesarios para las operaciones del organismo de evaluación de la conformidad, ni el uso de dichos sistemas de IA de alto riesgo para fines personales.***

5. Ni ***los organismos de evaluación de la conformidad, ni sus máximos directivos, ni el personal responsable de la realización de sus tareas de evaluación de la conformidad intervendrán directamente en el diseño, desarrollo, comercialización o utilización de sistemas de IA de alto riesgo, ni representarán a las partes que participan en estas actividades. No realizarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que hayan sido notificados. Esto se aplicará, en particular, a los servicios de consultoría.***

6. Los organismos notificados se organizarán y funcionarán de manera que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán y aplicarán una estructura y procedimientos para salvaguardar la imparcialidad y promover y aplicar los principios de imparcialidad en toda su organización, personal y actividades de evaluación.

7. 1. Los organismos notificados dispondrán de procedimientos documentados que garanticen que su personal, comités, filiales, subcontratistas y cualquier organismo asociado o personal de organismos externos mantienen, ***con arreglo al artículo 78,*** la confidencialidad de la información que obre en su poder durante la realización de las actividades de evaluación de la conformidad, salvo cuando la legislación exija su divulgación. El personal de los organismos notificados estará obligado a observar el secreto profesional acerca de toda la información recabada en el marco de sus tareas, salvo con respecto a las autoridades notificantes del Estado miembro en que realice sus actividades.

8. Los organismos notificados dispondrán de procedimientos para la realización de actividades que tengan debidamente en cuenta el tamaño del proveedor, el sector en el que opera, su estructura y el grado de complejidad del sistema de IA de que se trate.

9. Los organismos notificados suscribirán un seguro de responsabilidad civil apropiado para sus actividades de evaluación de la conformidad, a menos que la responsabilidad sea asumida por el Estado miembro ***en el que estén establecidos con arreglo al*** Derecho nacional o que el ***propio*** Estado miembro sea directamente responsable de la evaluación de la conformidad.

10. Los organismos notificados deberán ser capaces de desempeñar todas las tareas que les incumban en virtud del presente Reglamento con el máximo nivel de integridad profesional y con la competencia exigida en el ámbito específico, independientemente de que dichas tareas sean realizadas por los propios organismos notificados o en su nombre y bajo su responsabilidad.

11. Los organismos notificados dispondrán de competencias internas suficientes para poder evaluar eficazmente las tareas realizadas por partes externas en su nombre. ▌El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico***,*** ***jurídico*** y científico que posea experiencia y conocimientos en relación con los ***tipos*** pertinentes ***de sistemas*** de IA, datos e informática de datos, y en relación con los requisitos establecidos en la sección 2.

12. Los organismos notificados participarán en las actividades de coordinación contempladas en el artículo 38. Asimismo, participarán directamente o estarán representados en los organismos europeos de normalización, o se asegurarán de que conocen y están al día de las normas pertinentes.

Artículo 32

Presunción de conformidad con los requisitos relativos a los organismos notificados

Si un organismo de evaluación de la conformidad demuestra que cumple los criterios establecidos en las normas armonizadas pertinentes o partes de las mismas, cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea, se presumirá que cumple los requisitos establecidos en el artículo 31 en la medida en que las normas armonizadas aplicables cubran esos requisitos.

Artículo 33

Filiales de organismos notificados y subcontratación

1. 1. Cuando un organismo notificado subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplen los requisitos establecidos en el artículo 31 e informará a la autoridad notificante en consecuencia.

2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por subcontratistas o filiales.

3. Las actividades sólo podrán ser subcontratadas o realizadas por una filial con el acuerdo del proveedor. ***Los organismos notificados pondrán a disposición del público una lista de sus filiales.***

4. Los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial, así como el trabajo que estos realicen con arreglo al presente Reglamento***, se mantendrán a disposición de la autoridad notificante durante un período de cinco años a partir de la fecha de conclusión de la actividad de subcontratación***.

Artículo 34

Obligaciones operativas de los organismos notificados

1. *Los organismos notificados verificarán la conformidad de los sistemas de IA de alto riesgo con arreglo a los procedimientos de evaluación de la conformidad establecidos en el artículo 43.*

2. *Los organismos notificados evitarán cargas innecesarias a los proveedores en el ejercicio de sus actividades y tendrán debidamente en cuenta el tamaño del proveedor, el sector en el que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a minimizar las cargas administrativas y los costes de cumplimiento para las microempresas y las pequeñas empresas en el sentido de la Recomendación 2003/361/CE. No obstante, el organismo notificado respetará el grado de rigor y el nivel de protección necesarios para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento. .*

3. *Los organismos notificados pondrán a disposición de la autoridad notificante a que se refiere el artículo 28, y le presentarán cuando ésta lo solicite, toda la documentación pertinente, incluida la de los proveedores, para que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y para facilitar la evaluación a que se refiere la presente sección.*

Artículo 35

Números de identificación y listas de organismos notificados

1. La Comisión asignará un único número de identificación a cada organismo notificado, incluso cuando un organismo sea notificado con arreglo a más de un acto de la Unión.

2. La Comisión pondrá a disposición del público la lista de los organismos notificados en virtud del presente Reglamento, incluidos sus números de identificación y las actividades para las que han sido notificados. La Comisión velará por que la lista se mantenga actualizada.

Artículo 36

Cambios en las notificaciones

1. La autoridad notificante notificará a la Comisión y a los demás Estados miembros cualquier cambio pertinente en la notificación de un organismo notificado a través de la herramienta de notificación electrónica a que se refiere el artículo 30, apartado 2.

2. Los procedimientos establecidos en los artículos 29 y 30 se aplicarán a las ampliaciones del ámbito de aplicación de la notificación.

Para las modificaciones de la notificación que no sean ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados siguientes.

3. Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará a la autoridad notificante y a los proveedores afectados lo antes posible y, en caso de cese previsto, como mínimo un año antes del cese de sus actividades. Los certificados del organismo notificado podrán seguir siendo válidos durante un período temporal de nueve meses tras el cese de las actividades del organismo notificado, a condición de que otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad de los sistemas de IA de alto riesgo cubiertos por dichos certificados. Este último organismo notificado completará una evaluación completa de los sistemas de IA afectados antes de que finalice dicho período de nueve meses, antes de expedir nuevos certificados para dichos sistemas. Cuando el organismo notificado haya cesado su actividad, la autoridad notificante retirará la designación.

4. 1. Cuando una autoridad ***notificante tenga motivos suficientes para considerar*** que un organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o que no está cumpliendo sus obligaciones, investigará el asunto sin demora y con la máxima diligencia. En este contexto, informará al organismo notificado en cuestión de las objeciones planteadas y le ofrecerá la posibilidad de dar a conocer su punto de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado ▌ ya no cumple los requisitos establecidos en el artículo 31 o no está ***cumpliendo*** sus obligaciones, restringirá, suspenderá o retirará ▌ la designación, según el caso, dependiendo de la gravedad del incumplimiento ***de los requisitos u obligaciones***. Informará inmediatamente de ello a la Comisión y a los demás Estados miembros.

5. En caso de suspensión, restricción o retirada total o parcial de su designación, ***el organismo notificado informará de ello a los prestadores afectados a más tardar en un plazo de diez días.***

6. En caso de restricción, suspensión o retirada de una designación, la autoridad notificante adoptará las medidas oportunas para que se conserven los expedientes del organismo notificado en cuestión y para ponerlos a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado cuando éstas los soliciten.

7. En caso de restricción, suspensión o retirada de una designación, la autoridad notificante deberá:

(a) evaluar el impacto en los certificados expedidos por el organismo notificado;

(b) presentar un informe sobre sus conclusiones a la Comisión y a los demás Estados miembros en un plazo de tres meses a partir de la notificación de los cambios en la designación;

(c) exigir al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, los certificados que se hayan expedido indebidamente, con el fin de garantizar la conformidad permanente de los sistemas de IA en el mercado;

(d) informar a la Comisión y a los Estados miembros sobre los certificados cuya suspensión o retirada haya exigido;

(e) facilitará a las autoridades nacionales competentes del Estado miembro en el que el prestador tenga su domicilio social toda la información pertinente sobre los certificados cuya suspensión o retirada haya exigido; en caso necesario, dicha autoridad tomará las medidas oportunas para evitar un riesgo potencial para la salud, la seguridad o los derechos fundamentales.

8. ***Con excepción de los certificados expedidos indebidamente, y cuando una designación haya sido suspendida o restringida, los certificados seguirán siendo válidos en una de las siguientes circunstancias:***

(a) ***la autoridad notificante ha confirmado, en el plazo de un mes a partir de la suspensión o restricción, que no existe riesgo para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o restricción, y la autoridad notificante ha esbozado un calendario de actuaciones para subsanar la suspensión o restricción; o bien***

(b) ***la autoridad notificante ha confirmado que no se expedirá, modificará ni reexpedirá ningún certificado relacionado con la suspensión durante el transcurso de la suspensión o restricción, y declara si el organismo notificado tiene capacidad para seguir supervisando y seguir siendo responsable de los certificados existentes expedidos durante el período de suspensión o restricción; En caso de que la*** autoridad ***notificante determine que el organismo notificado no tiene capacidad para seguir supervisando los certificados existentes expedidos, el proveedor del sistema cubierto por el certificado confirmará por escrito a las autoridades nacionales competentes del Estado miembro en el que tenga su domicilio social, en un plazo de tres meses a partir de la suspensión o restricción, que otro organismo notificado cualificado está asumiendo temporalmente las funciones del organismo notificado para supervisar y seguir siendo responsable de los certificados durante el período de suspensión o restricción.***

9. Con excepción de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados seguirán siendo válidos durante un periodo de nueve meses en las siguientes circunstancias:

(a) la autoridad nacional competente del Estado miembro en el que tenga su domicilio social el proveedor del sistema de IA objeto del certificado haya confirmado que no existe ningún riesgo para la salud, la seguridad o los derechos fundamentales asociado a los sistemas de IA de alto riesgo de que se trate; y

(b) otro organismo notificado ha confirmado por escrito que asumirá inmediatamente la responsabilidad de evaluar dichos sistemas de IA y que completará su evaluación en un plazo de 12 meses a partir de la retirada de la designación.

En las circunstancias contempladas en el párrafo primero, la autoridad nacional competente del Estado miembro en el que tenga su sede el proveedor del sistema objeto del certificado podrá prorrogar la validez provisional de los certificados por períodos adicionales de tres meses, que no superarán los doce meses en total.

La autoridad nacional competente o el organismo notificado que asuma las funciones del organismo notificado afectado por el cambio de designación informará inmediatamente de ello a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

Artículo 37

Impugnación de la competencia de los organismos notificados

1. La Comisión investigará, en caso necesario, todos los casos en que existan razones para dudar ***de la competencia de*** un organismo notificado ***o del cumplimiento continuado por parte de un organismo notificado de*** los requisitos establecidos en el artículo 31 ***y de sus responsabilidades aplicables***.

2. La autoridad notificante facilitará a la Comisión, a petición de ésta, toda la información pertinente sobre la notificación ***o el mantenimiento de la competencia*** del organismo notificado en cuestión.

3. La Comisión velará por que toda la información ***sensible*** obtenida en el curso de sus investigaciones con arreglo al presente artículo sea tratada confidencialmente de ***conformidad con el artículo 78***.

4. Cuando la Comisión compruebe que un organismo notificado no cumple o ha dejado de cumplir los requisitos ***de su notificación***, ***informará*** al Estado miembro notificante ***al respecto y le pedirá*** que adopte las medidas correctoras necesarias, que pueden consistir, si es necesario, en la ***suspensión o*** retirada de ***la*** notificación***. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión podrá, mediante un acto de ejecución, suspender, restringir o retirar la designación***. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el apartado 2 del artículo 98.

Artículo 38

Coordinación de los organismos notificados

1. La Comisión velará por que, en lo que respecta a los ***sistemas de IA de alto riesgo,*** se establezcan y funcionen adecuadamente una coordinación y una cooperación adecuadas entre los organismos notificados activos en los procedimientos de evaluación de la conformidad ▌ con arreglo al presente Reglamento en forma de grupo sectorial de organismos notificados.

2. Cada ***autoridad notificante*** se asegurará de que los organismos que notifica participan en el trabajo del grupo mencionado en el apartado 1, directamente o a través de representantes designados.

3. La Comisión preverá el intercambio de conocimientos y mejores prácticas entre las autoridades de notificación de los Estados miembros.

Artículo 39

Organismos de evaluación de la conformidad de terceros países

Los organismos de evaluación de la conformidad establecidos con arreglo a la legislación de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a realizar las actividades de los organismos notificados con arreglo al presente Reglamento***, siempre que cumplan los requisitos del artículo 31 o garanticen un nivel de cumplimiento equivalente***.

Sección 5

Normas, evaluación de la conformidad, certificados, registro

Artículo 40

Normas armonizadas ***y resultados de la normalización***

1. Se presumirá que los sistemas de IA de alto riesgo que sean conformes con normas armonizadas o partes de las mismas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* ***de conformidad con el Reglamento (UE) no 1025/2012*** son conformes con los requisitos establecidos en la sección 2 del presente capítulo ***o, según proceda, con las obligaciones establecidas en el*** capítulo IV ***del presente Reglamento***, en la medida en que dichas normas cubran esos requisitos u obligaciones.

2. ***La Comisión emitirá solicitudes de normalización que cubran todos los requisitos establecidos en*** la sección 2 del presente capítulo y***,*** en su caso, ***las obligaciones establecidas en el*** capítulo ***IV del presente Reglamento, de conformidad con el artículo 10 del Reglamento (UE) no 1025/2012, sin demoras indebidas. En la solicitud de normalización también se pedirán resultados sobre los procesos de información y documentación para mejorar el rendimiento de los recursos de los sistemas de IA, como la reducción del consumo de energía y de otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, y sobre el desarrollo energéticamente eficiente de modelos de IA de propósito general. Al preparar una solicitud de normalización, la Comisión consultará al Consejo y a las partes interesadas pertinentes, incluido el foro consultivo.***

Al emitir una solicitud de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas han de ser claras, coherentes, incluidas las normas desarrolladas en los diversos sectores para los productos cubiertos por la legislación de armonización de la Unión existente enumerada en el anexo I, y destinadas a garantizar que los sistemas de IA o los modelos de IA comercializados o puestos en servicio en la Unión cumplen los requisitos pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de sus mejores esfuerzos para cumplir los objetivos mencionados en los párrafos primero y segundo del presente apartado, de conformidad con el artículo 24 del Reglamento (UE) no 1025/2012.

3. Los participantes en el proceso de normalización tratarán de promover la inversión y la innovación en la IA, incluso mediante el aumento de la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, y contribuirán a reforzar la cooperación mundial en materia de normalización y teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que sean coherentes con los valores, los derechos fundamentales y los intereses de la Unión, y potenciarán la gobernanza multilateral garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n.º 1025/2012.

Artículo 41

Especificaciones comunes

1. ***La Comisión estará facultada para adoptar actos de ejecución por los que se establezcan especificaciones comunes para los requisitos establecidos en*** la sección ***2 del presente capítulo o, en su caso, para las*** obligaciones establecidas en el capítulo IV***, cuando se cumplan las siguientes condiciones:***

   (a) la Comisión ha solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) no 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en la sección ***2 del presente capítulo, y:***

      (i) la solicitud no ha sido aceptada por ninguno de los organismos europeos de normalización; o

      (ii) las normas armonizadas que respondan a dicha solicitud no se entreguen en el plazo establecido de conformidad con el apartado 1 del artículo 10 del Reglamento (UE) n.º 1025/2012; o

      (iii) las normas armonizadas pertinentes no abordan suficientemente los problemas relacionados con los derechos fundamentales; o

      (iv) las normas armonizadas no se ajustan a lo solicitado; y

(b) no se ha publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que cubran los requisitos contemplados en la sección 2 del presente título, de conformidad con el Reglamento (UE) no 1025/2012, y no se espera que se publique tal referencia en un plazo razonable.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2, previa consulta al foro consultivo contemplado en el artículo 67.

2. Antes de preparar un proyecto de acto de ejecución, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 1 del presente artículo.

3. Se presumirá que los sistemas de IA de alto riesgo que sean conformes con las especificaciones comunes a que se refiere el apartado 1***, o con partes de dichas especificaciones,*** son conformes con los requisitos establecidos en la sección 2, en la medida en que dichas especificaciones comunes cubran dichos requisitos.

4. ***1. Cuando un organismo europeo de normalización adopte una norma armonizada y proponga a la Comisión la publicación de su referencia en el Diario Oficial de la Unión Europea, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) no 1025/2012. 2. Cuando se publique la referencia a una norma armonizada en el Diario Oficial de la Unión Europea, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o partes de los mismos que cubran los mismos requisitos establecidos en*** la sección ***2 del presente capítulo.***

5. Cuando los proveedores ***de sistemas de IA de alto riesgo*** no cumplan las especificaciones comunes mencionadas en el apartado 1, deberán justificar debidamente que han adoptado soluciones técnicas que ***cumplen los requisitos mencionados en*** la sección 2 ***a un nivel al*** menos equivalente a los mismos.

6. Cuando un Estado miembro considere que un pliego de condiciones común no cumple totalmente los requisitos establecidos en la sección ***2, informará de ello a la Comisión con una explicación detallada. La Comisión evaluará dicha información y, si procede, modificará el acto de ejecución por el que se establece el pliego de condiciones común de que se trate.***

Artículo 42

Presunción de conformidad con determinados requisitos

1. ▌Se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos ***que reflejen*** el entorno geográfico, conductual***, contextual o*** funcional específico en el que están destinados a ser utilizados cumplen los ***requisitos pertinentes*** establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya emitido una declaración de conformidad en virtud de un régimen de ciberseguridad con arreglo al Reglamento (UE) 2019/881 y cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea cumplen los requisitos de* ciberseguridad establecidos en el artículo 15 del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad o partes de los mismos cubran dichos requisitos.

Artículo 43

Evaluación de la conformidad

1. En el caso de los sistemas de IA de alto riesgo enumerados en el punto 1 del anexo III, cuando, al demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, el proveedor haya aplicado las normas armonizadas a que se refiere el artículo 40 o, en su caso, las especificaciones comunes a que se refiere el artículo 41, el proveedor ***optará por*** uno de los siguientes procedimientos de evaluación de la conformidad basados en:

   (a) el control interno contemplado en el Anexo VI; ***o***

   (b) la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, con la participación de un organismo notificado, contempladas en el anexo VII.

▌Al demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, el proveedor ***seguirá el procedimiento de evaluación de la conformidad establecido en el anexo VII, en el que:***

   (a) no existan las normas armonizadas a que se refiere el artículo 40 ▌ y no se disponga de las especificaciones comunes a que se refiere el artículo 41***;***

   (b) el proveedor ***no ha aplicado, o sólo ha aplicado parcialmente, la norma armonizada;***

   (c) existen las especificaciones comunes mencionadas en la letra a), pero el proveedor no las ha aplicado;

   (d) una o varias de las normas armonizadas mencionadas en la letra a) se hayan publicado con una restricción, y sólo en la parte de la norma que haya sido restringida.

A efectos del procedimiento de evaluación de la conformidad contemplado en el anexo VII, el proveedor podrá elegir cualquiera de los organismos notificados. No obstante, cuando el sistema de IA de alto riesgo esté destinado a ser puesto en servicio por autoridades policiales, de inmigración o asilo o por instituciones, órganos u organismos de la Unión, actuará como organismo notificado la autoridad de vigilancia del mercado a que se refiere el artículo 74, apartados 8 o 9, según proceda.

2. Para los sistemas de IA de alto riesgo contemplados en los puntos 2 a 8 del anexo III, los proveedores seguirán el procedimiento de evaluación de la conformidad basado en el control interno contemplado en el anexo VI, que no prevé la participación de un organismo notificado.

3. En el caso de los sistemas de IA de alto riesgo cubiertos por la legislación de armonización de la Unión enumerada en la sección A del anexo I, el proveedor seguirá el procedimiento de evaluación de la conformidad pertinente exigido en virtud de dichos actos jurídicos. Los requisitos establecidos en la sección 2 del presente capítulo se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. Puntos 4.3., 4.4.,
4.5. y el quinto párrafo del punto 4.6 del Anexo VII.

A efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo a dichos actos jurídicos tendrán derecho a controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en la sección 2, siempre que el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 10 y 11, haya sido evaluado en el contexto del procedimiento de notificación con arreglo a dichos actos jurídicos.

Cuando un acto jurídico enumerado en la sección A del anexo I permita al fabricante del producto renunciar a la evaluación de la conformidad por terceros, siempre que dicho fabricante haya aplicado todas las normas armonizadas que cubran todos los requisitos pertinentes, dicho fabricante sólo podrá hacer uso de esa opción si también ha aplicado las normas armonizadas o, en su caso, las especificaciones comunes a que se refiere el artículo 41, que cubran los requisitos establecidos en la sección 2 del presente capítulo.

4. Los sistemas de IA de alto riesgo ***que ya hayan sido sometidos a un procedimiento de evaluación de la conformidad*** deberán someterse a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, independientemente de si el sistema modificado está destinado a ser distribuido ulteriormente o sigue siendo utilizado por el ***implantador actual***.

   En el caso de los sistemas de IA de alto riesgo que sigan aprendiendo después de su comercialización o puesta en servicio, los cambios en el sistema de IA de alto riesgo y sus prestaciones que hayan sido determinados previamente por el proveedor en el momento de la evaluación inicial de la conformidad y formen parte de la información contenida en la documentación técnica a que se refiere el anexo IV, punto 2, letra f), no constituirán una modificación sustancial.

5. La Comisión adoptará actos delegados con arreglo al artículo 97 para actualizar los anexos VI y VII a la luz del progreso técnico.

6. La Comisión adoptará actos delegados con arreglo al artículo 97 por los que se modifiquen los apartados 1 y 2 del presente artículo con el fin de someter los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 2 a 8, al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes del mismo. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo VI para prevenir o reducir al mínimo los riesgos para la salud y la seguridad y la protección de los derechos fundamentales que plantean dichos sistemas, así como la disponibilidad de capacidades y recursos adecuados entre los organismos notificados.

Artículo 44
Certificados

1. Los certificados expedidos por los organismos notificados de conformidad con el Anexo VII se redactarán en ***una lengua fácilmente comprensible*** para las ***autoridades competentes del*** Estado miembro en el que esté establecido el organismo notificado**.**

2. Los certificados serán válidos durante el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el Anexo I ni de cuatro años para los sistemas de IA contemplados en el ***Anexo III***. A petición del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales, que no excederán de cinco años en ***el caso de los sistemas de IA incluidos en el Anexo I y de cuatro años en el caso de los sistemas de IA incluidos en el Anexo III***, sobre la base de una nueva evaluación realizada con arreglo a los procedimientos de evaluación de la conformidad aplicables. ***Todo suplemento de un certificado seguirá siendo válido siempre que el certificado al que complemente sea válido.***

3. Si un organismo notificado comprueba que un sistema de IA ya no cumple los requisitos establecidos en la sección 2, suspenderá o retirará el certificado expedido o le impondrá restricciones, teniendo en cuenta el principio de proporcionalidad, a menos que el proveedor del sistema garantice el cumplimiento de dichos requisitos mediante la adopción de medidas correctoras adecuadas en un plazo adecuado fijado por el organismo notificado. El organismo notificado motivará su decisión.

Deberá existir un procedimiento de recurso contra las decisiones de los organismos notificados, incluidos los certificados de conformidad expedidos.

Artículo 45

Obligaciones de información de los organismos notificados

1. Los organismos notificados informarán a la autoridad notificante de lo siguiente

(a) los certificados de evaluación de la documentación técnica de la Unión, los suplementos de dichos certificados y las aprobaciones de los sistemas de gestión de la calidad expedidos de conformidad con los requisitos del Anexo VII;

(b) cualquier denegación, restricción, suspensión o retirada de un certificado de evaluación de la documentación técnica de la Unión o de una aprobación de un sistema de gestión de la calidad expedidos de conformidad con los requisitos del anexo VII;

(c) cualquier circunstancia que afecte al alcance o a las condiciones de la notificación;

(d) cualquier solicitud de información que hayan recibido de las autoridades de vigilancia del mercado en relación con las actividades de evaluación de la conformidad;

(e) previa solicitud, las actividades de evaluación de la conformidad realizadas en el ámbito de su notificación y cualquier otra actividad realizada, incluidas las actividades transfronterizas y la subcontratación.

2. Cada organismo notificado informará a los demás organismos notificados de:

(a) las aprobaciones de sistemas de gestión de la calidad que haya denegado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido;

(b) Certificados de evaluación de la documentación técnica de la Unión o cualquier suplemento de los mismos que haya denegado, retirado, suspendido o restringido de otro modo y, previa solicitud, de los certificados y/o suplementos de los mismos que haya expedido.

3. Cada organismo notificado proporcionará a los demás organismos notificados que realicen actividades similares de evaluación de la conformidad que abarquen los mismos ***tipos de sistemas de IA*** información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de la evaluación de la conformidad.

4. Las obligaciones contempladas en los apartados 1, 2 y 3 del presente artículo se cumplirán de conformidad con el artículo 78.

Artículo 46

Excepción al procedimiento de evaluación de la conformidad

1. No obstante lo dispuesto en el artículo 43 y previa ***solicitud debidamente justificada***, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas específicos de IA de alto riesgo en el territorio del Estado miembro de que se trate, por razones excepcionales de seguridad pública o de protección de la vida y la salud de las personas, protección del medio ambiente o protección de activos industriales e infraestructurales clave. Dicha autorización tendrá una duración limitada ▌ mientras se llevan a cabo los procedimientos necesarios de evaluación de la conformidad, teniendo en cuenta ***las razones excepcionales que justifican la excepción***. La conclusión de dichos procedimientos se llevará a cabo sin demoras indebidas.

2. En una situación de urgencia debidamente justificada por razones excepcionales de seguridad pública o en caso de amenaza específica, sustancial e inminente para la vida o la seguridad física de personas físicas, las fuerzas y cuerpos de seguridad o las autoridades de protección civil podrán poner en servicio un sistema específico de IA de alto riesgo sin la autorización a que se refiere el apartado 1, siempre que dicha autorización se solicite durante o después de la utilización sin demora injustificada. Si se deniega la autorización a que se refiere el apartado 1, el uso del sistema de IA de alto riesgo cesará con efecto inmediato y todos los resultados y productos de dicho uso se desecharán inmediatamente.

3. La autorización a que se refiere el apartado 1 sólo se expedirá si la autoridad de vigilancia del mercado llega a la conclusión de que el sistema de IA de alto riesgo cumple los requisitos de la Sección

2. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida con arreglo al apartado 1. ***Esta obligación no cubrirá los datos operativos sensibles en relación con las actividades de las autoridades policiales.***

4. Cuando, en el plazo de 15 días naturales a partir de la recepción de la información mencionada en el apartado 3, ni un Estado miembro ni la Comisión hayan planteado objeciones a una autorización expedida por una autoridad de vigilancia del mercado de un Estado miembro de conformidad con el apartado 1, dicha autorización se considerará justificada.

5. Cuando, en un plazo de 15 días naturales a partir de la recepción de la notificación a que se refiere el apartado 3, un Estado miembro formule objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o cuando la Comisión considere que la autorización es contraria al Derecho de la Unión, o que la conclusión de los Estados miembros sobre la conformidad del sistema a que se refiere el apartado 3 es infundada, la Comisión iniciará sin demora consultas con el Estado miembro pertinente. Los operadores afectados serán consultados y tendrán la posibilidad de presentar sus puntos de vista. A la vista de las mismas, la Comisión decidirá si la autorización está justificada. La Comisión comunicará su decisión al Estado miembro interesado y a los operadores afectados.

6. Cuando la Comisión considere que la autorización no está justificada, la autoridad de vigilancia del mercado del Estado miembro en cuestión la retirará.

7. ▌Para los sistemas de IA de alto riesgo ***relacionados con productos*** cubiertos por la ***legislación de armonización de la Unión enumerada en la sección A del anexo I, solo se aplicarán*** las ***excepciones a la evaluación de la conformidad establecidas en dicha legislación de armonización de la Unión***.

Artículo 47

Declaración de conformidad de la UE

1. 1. El proveedor redactará una declaración UE de conformidad, ***legible por máquina y firmada física o electrónicamente,*** para cada sistema de IA de alto ***riesgo,*** y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a partir de la introducción en el mercado o la puesta en servicio del sistema de IA ***de alto riesgo***. En la declaración UE de conformidad se identificará el sistema de IA ***de alto riesgo*** para el que ha sido elaborada***.*** Previa solicitud, se ***presentará una*** copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes.

2. La declaración UE de conformidad afirmará que el sistema de IA de alto riesgo en cuestión cumple los requisitos establecidos en la sección 2. 2. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a ***una lengua fácilmente comprensible para*** las ***autoridades nacionales competentes de los*** Estados miembros en los que se introduzca en el ***mercado o se*** comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sujetos a otra legislación de armonización de la Unión que también requiera una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a toda la legislación de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para identificar la legislación de armonización de la Unión a la que se refiere la declaración.

4. Al elaborar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en la sección 2. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

5. La Comisión adoptará actos delegados con arreglo al artículo 97 para actualizar el contenido de la declaración UE de conformidad que figura en el anexo V, a fin de introducir los elementos que resulten necesarios a la luz del progreso técnico.

Artículo 48 Marcado CE

1. El marcado CE estará ***sujeto*** a los ***principios generales establecidos en el artículo 30 del Reglamento (CE) nº 765/2008***.

2. ***En el caso de los sistemas de IA de alto riesgo suministrados digitalmente, se utilizará un marcado CE digital, únicamente si se puede acceder fácilmente a él a través de la interfaz desde la que se accede a dicho sistema o a través de un código legible por máquina de fácil acceso u otro medio electrónico.***

3. El marcado CE ***se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando ello no sea posible o no pueda garantizarse debido a la naturaleza del sistema de IA de alto riesgo,*** se ***colocará*** en el ***embalaje o en la documentación adjunta, según proceda***.

4. En su caso, el marcado CE irá seguido del número de identificación del organismo notificado responsable de los procedimientos de evaluación de la conformidad establecidos en el artículo 43. El número de identificación ***del organismo notificado será colocado por el propio organismo o, siguiendo sus instrucciones, por el proveedor o su representante autorizado. El número de identificación*** se indicará asimismo en todo material de promoción en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos para el marcado CE.

5. ***Cuando los sistemas de IA de alto riesgo estén sujetos a otra legislación de la Unión que también prevea la colocación del marcado CE, éste indicará que el sistema de IA de alto riesgo también cumple los requisitos de esa otra legislación.***

Artículo 49

Registro

1. Antes de comercializar o poner en servicio un sistema de IA de alto riesgo ***enumerado en Anexo III, con excepción de los sistemas de IA de alto riesgo a*** que se refiere el ***punto 2 del Anexo III***, el proveedor o, en su caso, el representante autorizado ***se registr***ará ***a sí mismo y a su*** sistema en la base de datos de la UE a que se refiere el artículo 71.

2. ***Antes de comercializar o poner en servicio un sistema de IA para el que el proveedor haya llegado a la conclusión de que no es de alto riesgo con arreglo al artículo 6, apartado 3, dicho proveedor o, en su caso, el representante autorizado se registrará a sí mismo y a dicho sistema en la base de datos de la UE a que se refiere el artículo 71.***

3. ***Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo enumerados en el punto 2 del anexo III, los responsables del despliegue que sean autoridades, agencias u organismos públicos o personas que actúen en su nombre se registrarán, seleccionarán el sistema y registrarán su uso en la base de datos de la UE a que se refiere el artículo 71.***

4. ***En el caso de los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del Anexo III, en los ámbitos de la aplicación de la ley, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1, 2 y 3 del presente artículo se efectuará en una sección segura no pública de la base de datos de la UE a que se refiere el artículo 71 e incluirá únicamente la siguiente información, según proceda, a que se refiere:***

(a) los puntos 1 a 10 de la sección A del anexo VIII, a excepción de los puntos 5a, 7 y 8;

(b) sección C, puntos 1 a 3***, del anexo VIII,;***

(c) Sección B, ***puntos 1 a 5, y puntos 8 y 9 del Anexo VIII;***

(d) los puntos 1 a 3 y el punto 5 del anexo IX.

Sólo la Comisión y las autoridades nacionales mencionadas en el artículo 74, apartado 8, tendrán acceso a las secciones restringidas de la base de datos de la UE enumeradas en el párrafo primero del presente apartado.

5. Los sistemas de IA de alto riesgo contemplados en el punto 2 del anexo III se registrarán a escala nacional.

CAPÍTULO IV

OBLIGACIONES DE TRANSPARENCIA PARA LOS *PROVEEDORES E IMPLANTADORES DE* DETERMINADOS SISTEMAS DE AI

Artículo 50

Obligaciones de transparencia para proveedores y usuarios de determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar ***directamente*** con personas físicas se diseñen y desarrollen de forma que ***las*** personas físicas ***afectadas*** sean informadas de que están interactuando con un sistema de IA, a menos que ello resulte obvio desde el punto de vista ***de una persona física razonablemente bien informada, observadora y perspicaz, teniendo en cuenta*** las circunstancias y el contexto de uso. Esta obligación no se aplicará a los sistemas de IA autorizados por la ley para detectar, prevenir, investigar o enjuiciar delitos, ***sin perjuicio de las salvaguardias adecuadas para los derechos y libertades de terceros,*** a menos que dichos sistemas estén a disposición del público para denunciar un delito.

2. ***Los proveedores de sistemas de IA, incluidos los sistemas de IA de propósito general, que generen contenidos sintéticos de audio, imagen, vídeo o texto, garantizarán que los resultados del sistema de IA estén marcados en un formato legible por máquina y detectable como generado o manipulado artificialmente. Los proveedores garantizarán que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las especificidades y limitaciones de los diversos tipos de contenidos, los costes de aplicación y el estado de la técnica generalmente reconocido, tal como pueda reflejarse en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA realicen una función de asistencia para la edición estándar o no alteren sustancialmente los datos de entrada proporcionados por el usuario o la semántica de los mismos, o cuando estén autorizados por ley para detectar, prevenir, investigar o perseguir delitos penales.***

3. ***Los responsables del despliegue*** de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán a las personas físicas expuestas al mismo del funcionamiento del sistema, ***y tratarán los datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE)*** 2018/1725 ***y la Directiva (UE)*** 2016/680***, según proceda***. Esta obligación no se aplicará a los sistemas de IA utilizados para la ***categorización*** biométrica ***y el reconocimiento de emociones***, permitidos por la ley para detectar, prevenir o investigar infracciones penales***, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, y de conformidad con el Derecho de la Unión***.

4. ***Los implantadores*** de un sistema de IA que genere o manipule contenidos de imagen, audio o vídeo ***que constituyan una falsificación profunda, deberán revelar que el contenido ha sido generado o manipulado artificialmente. Esta obligación no se aplicará cuando el uso esté autorizado por la ley para detectar, prevenir, investigar o perseguir delitos. Cuando el contenido forme parte de una obra o programa evidentemente artístico, creativo, satírico o análogo de ficción, las obligaciones de transparencia establecidas en el presente apartado se limitarán a revelar la existencia de dicho contenido generado o manipulado de una manera adecuada que no obstaculice la visualización o el disfrute de la obra***.

Los usuarios de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público deberán revelar que el texto ha sido generado o manipulado artificialmente. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o perseguir delitos o ***cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial*** de la ***publicación del contenido***.

5. ***La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas afectadas de forma clara y distinguible a más tardar en el momento de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables.***

6. Los apartados 1 a 4 no afectarán a los requisitos y obligaciones establecidos en el capítulo III***, y se entenderán sin perjuicio de otras obligaciones de transparencia establecidas en la legislación de la Unión o nacional para los implantadores de sistemas de IA.***

7. ***La Oficina de AI 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 artificialmente. La Comisión estará facultada para adoptar actos de ejecución a fin de aprobar dichos códigos de prácticas de conformidad con el procedimiento establecido en el artículo 56, apartados 6, 7 y 8. Si considera que el código no es adecuado, la Comisión está facultada para adoptar un acto de ejecución en el que se especifiquen las normas comunes para la aplicación de dichas obligaciones de conformidad con el procedimiento de examen establecido en el apartado 2 del artículo 98***.

CAPÍTULO V
MODELOS DE AI DE PROPÓSITO GENERAL

Sección 1 Normas de clasificación

Artículo 51

Clasificación de los modelos de IA de propósito general como modelos de IA de propósito general con riesgo sistémico

1. Un modelo de IA de propósito general se clasificará como modelo de IA de propósito general con riesgo sistémico si cumple alguno de los siguientes requisitos:

(a) tiene capacidades de alto impacto evaluadas sobre la base de herramientas técnicas y metodologías apropiadas, incluidos indicadores y puntos de referencia;

(b) sobre la base de una decisión de la Comisión, de oficio o a raíz de una alerta cualificada de la comisión técnica científica, tiene unas capacidades o un impacto equivalentes a los establecidos en la letra a), habida cuenta de los criterios establecidos en el anexo XIII.

2. Se presumirá que un modelo de IA de propósito general tiene capacidades de alto impacto de conformidad con el apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento medida en FLOPs sea superior a 10^25.

3. La Comisión adoptará actos delegados de conformidad con el artículo 97 para modificar los umbrales enumerados en los apartados 2 y 3 del presente artículo, así como para complementar los puntos de referencia e indicadores a la luz de la evolución tecnológica, como las mejoras algorítmicas o el aumento de la eficiencia de los equipos informáticos, cuando sea necesario, para que dichos umbrales reflejen el estado de la técnica.

Artículo 52

Procedimiento

1. Cuando un modelo de IA de propósito general cumpla el requisito contemplado en el artículo 51, apartado 1, letra a), el proveedor correspondiente lo notificará a la Comisión sin demora y, en cualquier caso, en el plazo de dos semanas a partir del momento en que se cumpla dicho requisito o se tenga conocimiento de que se va a cumplir. Dicha notificación incluirá la información necesaria para demostrar que se ha cumplido el requisito pertinente. Si la Comisión tiene conocimiento de que un modelo de IA de propósito general presenta riesgos sistémicos de los que no ha sido notificada, podrá decidir designarlo como modelo con riesgo sistémico.

2. El proveedor de un modelo de IA de propósito general que cumpla el requisito contemplado en el artículo 51, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados para demostrar que, excepcionalmente, aunque cumpla dicho requisito, el modelo de IA de propósito general no presenta, debido a sus características específicas, riesgos sistémicos y, por tanto, no debe clasificarse como modelo de IA de propósito general con riesgo sistémico.

3. Cuando la Comisión llegue a la conclusión de que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y el proveedor pertinente no haya podido demostrar que el modelo de IA de propósito general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos, y el modelo de IA de propósito general se considerará un modelo de IA de propósito general con riesgo sistémico.

4. La Comisión podrá designar un modelo de IA de propósito general como modelo que presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada de la comisión técnica científica con arreglo al artículo 90, apartado 1, letra a), sobre la base de los criterios establecidos en el anexo XIII.

La Comisión adoptará actos delegados de conformidad con el artículo 97 para especificar y actualizar los criterios establecidos en el anexo XIII.

5. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de propósito general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de propósito general presenta riesgos sistémicos sobre la base de los criterios establecidos en el anexo XIII. Dicha solicitud deberá contener razones objetivas, detalladas y nuevas que hayan surgido desde la decisión de designación. Los proveedores podrán solicitar la reevaluación como muy pronto seis meses después de la decisión de designación. Cuando la Comisión, tras su reevaluación, decida mantener la designación como modelo de IA de propósito general con riesgo sistémico, los proveedores podrán solicitar una reevaluación como muy pronto seis meses después de dicha decisión.

6. La Comisión velará por que se publique una lista de modelos de IA de propósito general con riesgo sistémico y mantendrá dicha lista actualizada, sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

Sección 2

Obligaciones de los proveedores de modelos de IA de uso general

Artículo 53

Obligaciones de los proveedores de modelos de IA de uso general

1. Los proveedores de modelos de IA de uso general deberán:

(a) elaborará y mantendrá actualizada la documentación técnica del modelo, incluido su proceso de formación y ensayo y los resultados de su evaluación, que contendrá, como mínimo, los elementos establecidos en el anexo XI, con el fin de facilitarla, previa solicitud, a la Oficina de AI y a las autoridades nacionales competentes;

(b) elaborará, mantendrá actualizada y facilitará información y documentación a los proveedores de sistemas de IA que pretendan integrar el modelo de IA de propósito general en sus sistemas de IA. Sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, la información y la documentación deberán:

(i) permitir a los proveedores de sistemas de IA conocer bien las capacidades y limitaciones del modelo de IA de propósito general y cumplir sus obligaciones en virtud del presente Reglamento; y

(ii) contener, como mínimo, los elementos que figuran en el Anexo XII;

(c) establecer una política para cumplir con la legislación de la Unión en materia de derechos de autor y, en particular, para identificar y cumplir, incluso a través de las tecnologías más avanzadas, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

(d) elaborar y poner a disposición del público un resumen suficientemente detallado sobre el contenido utilizado para el entrenamiento del modelo de IA de propósito general, de acuerdo con una plantilla facilitada por la Oficina de IA.

2. Las obligaciones establecidas en el apartado 1, letras a) y b), no se aplicarán a los proveedores de modelos de IA que se publiquen bajo una licencia libre y abierta que permita el acceso, el uso, la modificación y la distribución del modelo, y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de propósito general con riesgos sistémicos.

3. Los proveedores de modelos de IA de propósito general cooperarán en la medida necesaria con la Comisión y las autoridades nacionales competentes en el ejercicio de sus competencias y facultades con arreglo al presente Reglamento.

4. Los proveedores de modelos de IA de propósito general podrán basarse en códigos de buenas prácticas en el sentido del artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. Se presumirá que los proveedores que cumplan una norma europea armonizada cumplen las obligaciones establecidas en el apartado 1 del presente artículo. Los proveedores de modelos de IA de propósito general que no se adhieran a un código de buenas prácticas aprobado deberán demostrar medios de cumplimiento alternativos adecuados para su aprobación por la Comisión.

5. Con el fin de facilitar el cumplimiento del anexo XI, en particular las letras d) y e) del punto 2

(e) la Comisión adoptará actos delegados de conformidad con el artículo 97 para detallar las metodologías de medición y cálculo con vistas a permitir una documentación comparable y verificable.

6. La Comisión adoptará actos delegados con arreglo al artículo 97, apartado 2, para modificar los anexos XI y XII a la luz de la evolución tecnológica.

7. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 54

Representantes autorizados de proveedores de modelos de IA de uso general

1. Antes de introducir un modelo de IA de uso general en el mercado de la Unión, los proveedores establecidos en terceros países deberán designar, mediante mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. El prestador permitirá a su representante autorizado realizar las tareas especificadas en el mandato recibido del prestador.

2. El representante autorizado realizará las tareas especificadas en el mandato recibido del proveedor. Facilitará una copia del mandato a la Oficina de AI, a petición de ésta, en una de las lenguas oficiales de las instituciones de la Unión. A efectos del presente Reglamento, el mandato facultará al representante autorizado para llevar a cabo las siguientes tareas:

(a) comprobar que se ha elaborado la documentación técnica especificada en el Anexo XI y que el proveedor ha cumplido todas las obligaciones contempladas en los artículos 53 y, en su caso, 55;

(b) conservar una copia de la documentación técnica especificada en el anexo XI a disposición de la Oficina de IA y de las autoridades nacionales competentes, durante un período de 10 años a partir de la comercialización del modelo de IA de uso general, y mantener actualizados los datos de contacto del proveedor que designó al representante autorizado;

(c) facilitar a la Oficina de AI, previa solicitud motivada, toda la información y documentación, incluida la mencionada en la letra b), necesaria para demostrar su cumplimiento de las obligaciones del presente capítulo;

(d) cooperar con la Oficina de IA y las autoridades nacionales competentes, previa solicitud motivada, en cualquier acción que estas últimas emprendan en relación con un modelo de IA de propósito general con riesgos sistémicos, incluso cuando el modelo se integre en sistemas de IA comercializados o puestos en servicio en la Unión.

3. El mandato facultará al representante autorizado para que, además del proveedor o en su lugar, la Oficina de AI o las autoridades nacionales competentes se dirijan a él en todas las cuestiones relacionadas con el cumplimiento del presente Reglamento.

4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor actúa de forma contraria a sus obligaciones en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de AI de la terminación del mandato y de los motivos de la misma.

5. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de propósito general que se publiquen con arreglo a una licencia de fuente abierta y gratuita que permita el acceso, el uso, la modificación y la distribución del modelo, y cuyos parámetros, incluidas las ponderaciones, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, a menos que los modelos de IA de propósito general presenten riesgos sistémicos.

Sección 3

Obligaciones de los proveedores de modelos de IA de propósito general con riesgo sistémico

Artículo 55

Obligaciones de los proveedores de modelos de IA de propósito general con riesgo sistémico

1. Además de las obligaciones enumeradas en el artículo 53, los proveedores de modelos de IA de propósito general con riesgo sistémico deberán:

(a) realizar la evaluación del modelo de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, incluida la realización y documentación de pruebas contradictorias del modelo con vistas a identificar y mitigar el riesgo sistémico;

(b) evaluar y mitigar los posibles riesgos sistémicos a escala de la Unión, incluidas sus fuentes, que puedan derivarse del desarrollo, la comercialización o el uso de modelos de IA de propósito general con riesgo sistémico;

(c) hacer un seguimiento, documentar y comunicar sin demora indebida a la Oficina de AI y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctivas para hacerles frente;

(d) garantizar un nivel adecuado de protección de ciberseguridad para el modelo de IA de propósito general con riesgo sistémico y la infraestructura física del modelo.

2. Los proveedores de modelos de IA de propósito general con riesgo sistémico podrán basarse en códigos de prácticas en el sentido del artículo ***56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. Se presumirá que los proveedores que cumplan una norma europea armonizada cumplen las obligaciones establecidas en el apartado 1 del presente artículo. Los proveedores de modelos de IA de propósito general con riesgos sistémicos que no se adhieran a un código de buenas prácticas aprobado deberán demostrar medios de cumplimiento alternativos adecuados para su aprobación por la Comisión.***

3. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 56

Códigos de buenas prácticas

1. La Oficina de AI fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión para contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.

2. La Oficina de AI y el Consejo procurarán que los códigos de buenas prácticas cubran al menos las obligaciones previstas en los artículos 53 y 55, incluidas las siguientes cuestiones:

(a) medios para garantizar que la información a que se refieren las letras a) y b) del apartado 1 del artículo 53 se ***mantiene actualizada a la luz de la evolución del mercado y de la tecnología;***

(b) el nivel de detalle adecuado para el resumen sobre el contenido utilizado para la formación;

(c) la identificación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes, cuando proceda;

(d) las medidas, procedimientos y modalidades para la evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionados a los riesgos, tomarán en consideración su gravedad y probabilidad y tendrán en cuenta los retos específicos de hacer frente a esos riesgos a la luz de las posibles formas en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.

3. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán apoyar el proceso.

4. La Oficina de AI y el Consejo tratarán de garantizar que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, incluidos indicadores clave de rendimiento, según proceda, para garantizar la consecución de dichos objetivos, y que tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.

5. La Oficina de AI tratará de garantizar que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de AI sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, incluidos los medidos en relación con los indicadores clave de rendimiento, según proceda. Los indicadores clave de rendimiento y los compromisos de información reflejarán las diferencias de tamaño y capacidad entre los distintos participantes.

6. La Oficina AI y el Consejo supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Oficina AI y el Consejo evaluarán si los códigos de buenas prácticas cubren las obligaciones previstas en los artículos 53 y 55, así como las cuestiones enumeradas en el apartado 2 del presente artículo, y supervisarán y evaluarán periódicamente la consecución de sus objetivos. Publicarán su evaluación de la adecuación de los códigos de buenas prácticas.

La Comisión podrá, mediante un acto de ejecución, aprobar un código de buenas prácticas y darle una validez general en la Unión. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el apartado 2 del artículo 98.

7. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de propósito general a adherirse a los códigos de buenas prácticas. Para los proveedores de modelos de IA de propósito general que no presenten riesgos sistémicos, esta adhesión podrá limitarse a las obligaciones previstas en el artículo 53, a menos que declaren explícitamente su interés por adherirse al código completo.

8. La Oficina de AI también fomentará y facilitará, según proceda, la revisión y adaptación de los códigos de buenas prácticas, en particular a la luz de las normas que vayan surgiendo. La Oficina de AI colaborará en la evaluación de las normas disponibles.

9. Los códigos de buenas prácticas estarán listos a más tardar ... [nueve meses después de la fecha de entrada en vigor del presente Reglamento]. La Oficina de AI tomará las medidas necesarias, incluida la invitación a los proveedores con arreglo al apartado 7.

Si, a más tardar ... [12 meses a partir de la fecha de entrada en vigor], no puede ultimarse un código de buenas prácticas, o si la Oficina de AI lo considera inadecuado tras su evaluación ***con arreglo al apartado 6 del presente artículo, la Comisión podrá establecer, mediante actos de ejecución, normas comunes para la aplicación de las obligaciones previstas en los artículos 53 y 55, incluidas las cuestiones establecidas en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.***

CAPÍTULO VI
MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 57

Cajas de arena reguladoras de la IA

1. ***Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio aislado de regulación de la IA a nivel nacional**, **que estará operativo a más tardar el ... [24 meses a partir de la fecha de entrada en vigor del presente Reglamento]. Este espacio aislado también podrá establecerse conjuntamente con las autoridades competentes de uno o más Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento e instrumentos para la creación y el funcionamiento de los entornos aislados de regulación de la IA.***

   ***La obligación prevista en el párrafo primero también podrá cumplirse mediante la participación en un arenero existente, en la medida en que dicha participación proporcione un nivel equivalente de cobertura nacional para los Estados miembros participantes**.*

2. También podrán crearse otros espacios aislados de regulación de la IA a nivel regional o local, o establecidos conjuntamente con las autoridades competentes de otros Estados miembros.

3. El Supervisor Europeo de Protección de Datos también podrá establecer un espacio aislado de regulación de la IA para las instituciones, órganos y organismos de la Unión, y podrá ejercer las funciones y tareas de las autoridades nacionales competentes de conformidad con el presente capítulo.

4. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 2 asignen recursos suficientes para dar cumplimiento al presente artículo de manera eficaz y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA. El presente artículo no afectará a otros espacios aislados de regulación establecidos en virtud del Derecho de la Unión o nacional. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros entornos aislados y las autoridades nacionales competentes.

5. ***Los entornos aislados de regulación de la IA establecidos con arreglo al apartado 1 proporcionarán un entorno controlado que fomente la innovación y facilite el desarrollo, la formación, las pruebas y la validación de los sistemas innovadores de IA durante un tiempo limitado antes de su comercialización o puesta en servicio de conformidad con un plan específico del entorno aislado acordado entre los posibles proveedores y la autoridad competente. Estos "sandboxes" reglamentarios pueden incluir pruebas en condiciones del mundo real supervisadas en el "sandbox".***

6. ***Las autoridades competentes proporcionarán, según proceda, orientación, supervisión y apoyo en el marco del espacio aislado de regulación de la IA con vistas a identificar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, los ensayos, las medidas de mitigación y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, en su caso, de otra legislación de la Unión y de los Estados miembros supervisada en el marco del espacio aislado.***

7. ***Las autoridades competentes proporcionarán a los proveedores y posibles proveedores*** que utilicen el espacio aislado de regulación de la IA ***orientaciones sobre las expectativas en materia de regulación y sobre cómo cumplir los requisitos y obligaciones establecidos en el presente Reglamento.***

A petición del proveedor o posible proveedor del sistema de IA, la autoridad competente facilitará una prueba escrita de las actividades realizadas con éxito en el espacio aislado. La autoridad competente facilitará asimismo un informe de salida en el que se detallen las actividades realizadas en el espacio aislado y los resultados y enseñanzas correspondientes. Los proveedores podrán utilizar dicha documentación para demostrar su cumplimiento del presente Reglamento a través del proceso de evaluación de la conformidad o de las actividades pertinentes de vigilancia del mercado. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán positivamente en cuenta los informes de salida y la prueba escrita facilitados por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

8. *Sin perjuicio de las disposiciones en materia de confidencialidad del artículo 78, y con el acuerdo del proveedor o posible proveedor, la Comisión y la Junta estarán autorizadas a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones con arreglo al presente Reglamento. Si tanto el proveedor o posible proveedor como la autoridad nacional competente están de acuerdo explícitamente, el informe de salida podrá ponerse a disposición del público a través de la plataforma única de información a que se refiere el presente artículo.*

9. *La creación de espacios aislados de regulación de la IA deberá contribuir a la consecución de los siguientes objetivos:*

   (a) *mejorar la seguridad jurídica para lograr el cumplimiento normativo del presente Reglamento o, en su caso, del resto del Derecho de la Unión y nacional aplicable;*

(b) apoyar el intercambio de buenas prácticas mediante la cooperación con las autoridades que participan en el espacio aislado de regulación de la IA;

(c) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de IA;

(d) contribuir al aprendizaje normativo basado en pruebas;

(e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los suministran las PYME, incluidas las empresas de nueva creación.

10. ***Las autoridades nacionales competentes*** velarán por que***,*** en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o entren de otro modo en el ámbito de supervisión de otras autoridades nacionales o autoridades competentes que faciliten o apoyen el acceso a los datos, las autoridades nacionales de protección de datos y esas otras autoridades nacionales o competentes estén asociadas al funcionamiento del espacio aislado regulador de la IA ***y participen en la supervisión de esos aspectos en la medida de sus respectivas funciones y competencias***.

11. Los espacios aislados de regulación de la IA no afectarán a los poderes de supervisión o corrección de las autoridades competentes ***que supervisan los espacios aislados, incluso a nivel regional o local***. Cualquier riesgo significativo para la salud y la seguridad y los derechos fundamentales que se detecte durante el desarrollo y las pruebas de dichos sistemas de ***IA dará lugar a una*** mitigación adecuada***. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de ensayo, o la participación*** en el sandbox ***si no es posible una mitigación eficaz, e informarán a la Oficina de la IA de tal decisión. Las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites de*** la ***legislación pertinente, haciendo uso de sus facultades discrecionales cuando apliquen disposiciones legales con respecto a un proyecto específico de espacio aislado de IA, con el objetivo de apoyar la innovación en IA en la Unión***.

12. ***Los proveedores y posibles proveedores*** que participen en el espacio aislado de regulación de la IA seguirán siendo responsables, en virtud de la legislación de la Unión y nacional aplicable en materia de responsabilidad, de cualquier ***daño*** causado a terceros como consecuencia ***de*** la experimentación que tenga lugar en el espacio aislado. No ***obstante, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones de la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracción del presente Reglamento. En la medida en que otras autoridades competentes responsables de otro Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA en el espacio aislado y hayan proporcionado orientaciones para su cumplimiento, no se impondrán multas administrativas en relación con dicho Derecho.***

13. ***Los espacios aislados de regulación de la IA se diseñarán y aplicarán de forma que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.***

14. Las autoridades ***nacionales*** competentes ▌ coordinarán sus actividades y cooperarán en el marco del Consejo ▌. ▌

15. ***Las autoridades nacionales competentes informarán a la Oficina de Inteligencia Artificial y al Consejo de la creación de un espacio aislado y podrán solicitarle apoyo y orientación. La Oficina de la IA pondrá a disposición del público una lista de los compartimentos estancos de la IA previstos y existentes y la mantendrá actualizada para fomentar una mayor interacción en los compartimentos estancos de regulación de la IA y la cooperación transfronteriza.***

16. ***Las autoridades nacionales competentes presentarán a la Oficina de la IA y al Consejo informes anuales, comenzando un año después de la creación del espacio aislado regulador de la IA y, a continuación, cada año hasta su finalización, así como un informe final. Dichos informes contendrán información sobre los avances y resultados de la aplicación de esos espacios aislados, incluidas las mejores prácticas, los incidentes, las lecciones aprendidas y las recomendaciones sobre su configuración y, en su caso, sobre la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y sobre la aplicación de otros actos legislativos de la Unión supervisados por las autoridades competentes dentro del espacio aislado. Las autoridades nacionales competentes pondrán a disposición del público, en línea, dichos informes anuales o resúmenes de los mismos. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones con arreglo al presente Reglamento.***

17. La ***Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los entornos aislados reguladores de la IA para permitir a las partes interesadas interactuar con los entornos aislados reguladores de la IA y plantear preguntas a las autoridades competentes, así como solicitar orientaciones no vinculantes sobre la conformidad de los productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 62, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda***.

Artículo 58

Disposiciones detalladas y funcionamiento de los espacios aislados de regulación de la IA

1. Para evitar la fragmentación en toda la Unión, la Comisión adoptará actos de ejecución que especifiquen las disposiciones detalladas para el establecimiento, desarrollo, aplicación, funcionamiento y supervisión de los espacios aislados de regulación de la IA. Los actos de ejecución incluirán principios comunes sobre las siguientes cuestiones:

(a) criterios de admisibilidad y selección para participar en el espacio aislado de regulación de la IA;

(b) procedimientos para la solicitud, participación, supervisión, salida y finalización del espacio aislado de regulación de la IA, incluido el plan del espacio aislado y el informe de salida;

(c) las condiciones aplicables a los participantes.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

2. Los actos de ejecución a que se refiere el apartado 1 garantizarán que:

(a) Los espacios aislados de regulación de la IA están abiertos a cualquier proveedor potencial de un sistema de IA que cumpla los criterios de admisibilidad y selección, que serán transparentes y justos, y las autoridades nacionales competentes informarán a los solicitantes de su decisión en un plazo de tres meses a partir de la solicitud;

(b) Los espacios aislados de regulación de la IA permiten un acceso amplio e igualitario y se mantienen al día con la demanda de participación; los posibles proveedores también pueden presentar solicitudes en asociación con usuarios y otros terceros pertinentes;

(c) las disposiciones detalladas y las condiciones relativas a los compartimentos estancos reguladores de la IA apoyen en la mayor medida posible la flexibilidad de las autoridades nacionales competentes para establecer y gestionar sus compartimentos estancos reguladores de la IA;

(d) el acceso a los espacios aislados de regulación de la IA es gratuito para las PYME, incluidas las de nueva creación, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de manera justa y proporcionada;

(e) facilitan a los futuros proveedores, mediante los resultados de aprendizaje de los entornos aislados de regulación de la IA, el cumplimiento de las obligaciones de evaluación de la conformidad con arreglo al presente Reglamento y la aplicación voluntaria de los códigos de conducta a que se refiere el artículo 95;

(f) Los espacios aislados de regulación de la IA facilitan la participación de otros agentes relevantes dentro del ecosistema de la IA, como organismos notificados y organizaciones de normalización, PYME, empresas de nueva creación, empresas, innovadores, instalaciones de ensayo y experimentación, laboratorios de investigación y experimentación y Centros Europeos de Innovación Digital, centros de excelencia, investigadores individuales, con el fin de permitir y facilitar la cooperación con los sectores público y privado;

(g) los procedimientos, procesos y requisitos administrativos para la solicitud, selección, participación y salida del espacio aislado regulador de la IA sean sencillos, fácilmente inteligibles y se comuniquen con claridad para facilitar la participación de las PYME, incluidas las nuevas empresas, con capacidades jurídicas y administrativas limitadas, y se racionalicen en toda la Unión, a fin de evitar la fragmentación y que la participación en un espacio aislado regulador de la IA establecido por un Estado miembro o por el Supervisor Europeo de Protección de Datos se reconozca mutua y uniformemente y tenga los mismos efectos jurídicos en toda la Unión;

(h) la participación en el espacio aislado de regulación de la IA se limita a un periodo adecuado a la complejidad y escala del proyecto, que puede ser ampliado por la autoridad nacional competente;

(i) Los espacios aislados de regulación de la IA facilitan el desarrollo de herramientas e infraestructuras para probar, comparar, evaluar y explicar las dimensiones de los sistemas de IA relevantes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como las medidas para mitigar los riesgos para los derechos fundamentales y la sociedad en general.

3. Cuando proceda, se dirigirá a los posibles proveedores de los espacios aislados de regulación de la IA, en particular las PYME y las empresas de nueva creación, a los servicios previos al despliegue, como la orientación sobre la aplicación del presente Reglamento, a otros servicios de valor añadido, como la ayuda con los documentos de normalización y la certificación, las instalaciones de ensayo y experimentación, los Centros Europeos de Innovación Digital y los centros de excelencia.

4. Cuando las autoridades nacionales competentes consideren la posibilidad de autorizar ensayos en condiciones del mundo real supervisados en el marco de un espacio aislado de regulación de la IA que se establezca con arreglo al presente artículo, acordarán específicamente con los participantes las condiciones de dichos ensayos y, en particular, las salvaguardias adecuadas con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con vistas a garantizar prácticas coherentes en toda la Unión.

Artículo 59

Tratamiento adicional de datos personales para el desarrollo de determinados sistemas de IA de interés público en el espacio aislado de regulación de la IA

1. Los datos personales recogidos legalmente para otros fines ***podrán*** tratarse en un espacio aislado de regulación de la IA con el ***único*** fin de desarrollar***, formar*** y probar determinados sistemas de IA en el espacio aislado ***cuando se cumplan todas las*** condiciones siguientes:

(a) ▌ Los sistemas de IA serán desarrollados para salvaguardar intereses públicos sustanciales ***por una autoridad pública u otra persona física o jurídica y*** en uno o varios de los ámbitos siguientes:

(i) seguridad y salud públicas, incluida la ***detección y el diagnóstico de*** enfermedades

prevención, control y tratamiento ***y mejora de los sistemas sanitarios***;

(ii) un alto nivel de protección y mejora de la calidad del medio ambiente***, protección de la biodiversidad, protección contra la contaminación, medidas de transición ecológica, mitigación del cambio climático y medidas de adaptación***;

(iii) sostenibilidad energética;

(iv) seguridad y resistencia de los sistemas de transporte y movilidad, infraestructuras críticas y redes;

(v) eficiencia y calidad de la administración y los servicios públicos;

(b) los datos tratados son necesarios para cumplir uno o varios de los requisitos contemplados en el capítulo III, sección 2, cuando dichos requisitos no puedan cumplirse efectivamente mediante el tratamiento de datos anónimos, sintéticos u otros datos no personales;

(c) existan mecanismos de control eficaces para determinar si existen riesgos elevados para los ***derechos y libertades*** de los interesados***, tal como se contempla en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725,*** puedan surgir durante la experimentación del sandbox, así como mecanismos de respuesta para mitigar rápidamente esos riesgos y, en su caso, detener el tratamiento;

(d) todos los datos personales que vayan a tratarse en el contexto del sandbox se encuentren en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control del ***futuro proveedor,*** y sólo las personas autorizadas tengan acceso a ***dichos*** datos;

(e) ***Los proveedores pueden compartir los datos recogidos originalmente sólo en cumplimiento de la legislación de protección de datos de la Unión;*** ningún dato personal ***creado en el sandbox puede compartirse fuera de él;***

(f) cualquier tratamiento de datos personales en el contexto del sandbox no da lugar a medidas o decisiones que afecten a los interesados ***ni afecta a la aplicación de sus derechos establecidos en la legislación de la Unión sobre protección de datos personales***;

(g) todos los datos personales tratados en el contexto del sandbox se ***protegen mediante medidas técnicas y organizativas adecuadas y se*** suprimen una vez que la participación en el sandbox ha finalizado o los datos personales han alcanzado el final de su período de conservación;

(h) los registros del tratamiento de datos personales en el contexto del sandbox se conservan mientras dure la participación en el sandbox***, salvo disposición en contrario del Derecho de*** la Unión o nacional;

(i) se conserve una descripción completa y detallada del proceso y la justificación de la formación, las pruebas y la validación del sistema de IA, junto con los resultados de las pruebas, como parte de la documentación técnica mencionada en el anexo IV;

(j) se publique en el sitio web de las autoridades competentes un breve resumen del proyecto de IA desarrollado en el espacio aislado, sus objetivos y resultados previstos; ***esta obligación no cubrirá los datos operativos sensibles en relación con las actividades de las autoridades policiales, de control de fronteras, inmigración o asilo.***

2. ***2. A efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección contra amenazas a la seguridad pública y la prevención de las mismas, bajo el control y la responsabilidad de las autoridades policiales, el tratamiento de datos personales en los entornos aislados de regulación de la IA se basará en un Derecho específico o de la Unión o nacional y estará sujeto a las mismas condiciones acumulativas a que se refiere el apartado 1.***

3. El apartado 1 se entenderá sin perjuicio del Derecho de la Unión o nacional que excluya el tratamiento de datos personales para fines distintos de los explícitamente mencionados en dicho Derecho***, así como del Derecho de la Unión o nacional que establezca la base para el tratamiento de datos personales que sea necesario a efectos de desarrollo, prueba o formación de sistemas innovadores de IA o cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales***.

Artículo 60

Pruebas de sistemas de IA de alto riesgo en condiciones del mundo real fuera de los "cajones de arena" reguladores de la IA.

1. ***Los proveedores o posibles proveedores de sistemas de IA de alto riesgo enumerados en el anexo III podrán realizar pruebas de sistemas de IA de alto riesgo en condiciones del mundo real fuera de los entornos aislados reguladores de la IA, de conformidad con el presente artículo y el plan de pruebas en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.***

Los elementos detallados del plan de ensayos en condiciones reales se especificarán en actos de ejecución adoptados por la Comisión de conformidad con el procedimiento de examen contemplado en el artículo 98, apartado 2.

Esta disposición se entenderá sin perjuicio de la legislación de la Unión o nacional relativa a los ensayos en condiciones reales de los sistemas de IA de alto riesgo relacionados con los productos cubiertos por la legislación de armonización de la Unión enumerada en el anexo I.

2. ***Los proveedores o posibles proveedores podrán realizar pruebas de los sistemas de IA de alto riesgo contemplados en el anexo III en condiciones del mundo real en cualquier momento antes de la comercialización o puesta en servicio del sistema de IA por sí mismos o en asociación con uno o varios posibles implantadores.***

3. Los ensayos de sistemas de IA de alto riesgo en condiciones reales con arreglo al presente artículo se realizarán sin perjuicio de cualquier revisión ética que exija la legislación de la Unión o nacional.

4. Los proveedores o posibles proveedores sólo podrán realizar las pruebas en condiciones reales cuando se cumplan todas las condiciones siguientes:

(a) el proveedor o posible proveedor haya elaborado un plan de pruebas en condiciones reales y lo haya presentado a la autoridad de vigilancia del mercado del Estado miembro en el que vayan a realizarse las pruebas en condiciones reales;

(b) la autoridad de vigilancia del mercado del Estado miembro en el que vayan a realizarse los ensayos en condiciones reales haya aprobado los ensayos en condiciones reales y el plan de ensayos en condiciones reales. Cuando la autoridad de vigilancia del mercado no haya dado una respuesta en un plazo de 30 días, se entenderá que las pruebas en condiciones reales y el plan de pruebas en condiciones reales han sido aprobados. Cuando la legislación nacional no prevea una aprobación tácita, los ensayos en condiciones reales seguirán estando sujetos a una autorización;

(c) el proveedor o futuro proveedor, con excepción de los proveedores o futuros proveedores de sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III en los ámbitos de la aplicación de la ley, la migración, el asilo y la gestión de los controles fronterizos, y de los sistemas de IA de alto riesgo a que se refiere el punto 2 del anexo III, haya registrado los ensayos en condiciones reales en la parte no pública de la base de datos de la UE a que se refiere el artículo 71, apartado 3, con un número de identificación único para toda la Unión y con la información especificada en el anexo IX;

(d) el proveedor o posible proveedor que realice las pruebas en condiciones reales esté establecido en la Unión o haya designado a un representante legal que esté establecido en la Unión;

(e) los datos recogidos y tratados a efectos de las pruebas en condiciones reales sólo se transferirán a terceros países si se aplican las garantías adecuadas y aplicables en virtud del Derecho de la Unión;

(f) las pruebas en condiciones reales no duren más de lo necesario para alcanzar sus objetivos y, en cualquier caso, no superen los seis meses, prorrogables por un período adicional de seis meses, previa notificación del proveedor a la autoridad de vigilancia del mercado, acompañada de una explicación de la necesidad de dicha prórroga;

(g) los sujetos de las pruebas en condiciones del mundo real que sean ***personas vulnerables debido a su edad, discapacidad física o mental, estén debidamente protegidos;***

(h) cuando un proveedor o posible proveedor organice los ensayos en condiciones reales en cooperación con uno o varios implantadores o posibles implantadores, estos últimos hayan sido informados de todos los aspectos de los ensayos que sean pertinentes para su decisión de participar y hayan recibido las instrucciones pertinentes para el uso del sistema de IA a que se refiere el artículo 13; el proveedor o posible proveedor y el posible implantador celebrarán un acuerdo en el que se especifiquen sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a los ensayos en condiciones reales con arreglo al presente Reglamento y a otros actos legislativos nacionales y de la Unión aplicables;

(i) los sujetos de la prueba en condiciones del mundo real hayan dado su consentimiento informado de conformidad con el artículo 61, o en el caso de las fuerzas y cuerpos de seguridad, cuando la solicitud del consentimiento informado impida la prueba del sistema de IA, la propia prueba y el resultado de la prueba en condiciones del mundo real no tendrán ningún efecto negativo en los sujetos, y sus datos personales se suprimirán una vez realizada la prueba;

(j) los ensayos en condiciones reales sean supervisados eficazmente por el proveedor o posible proveedor, así como por los encargados del despliegue o posibles encargados del despliegue a través de personas debidamente cualificadas en el ámbito pertinente y que tengan la capacidad, formación y autoridad necesarias para desempeñar sus tareas;

(k) las predicciones, recomendaciones o decisiones del sistema de IA pueden ser efectivamente anuladas e ignoradas.

5. Cualquier sujeto de las pruebas en condiciones reales, o su representante legalmente designado, según proceda, podrá, sin perjuicio alguno y sin tener que aportar justificación alguna, retirarse de las pruebas en cualquier momento revocando su consentimiento informado y podrá solicitar la supresión inmediata y permanente de sus datos personales. La revocación del consentimiento informado no afectará a la licitud ni a la validez de las actividades ya realizadas.

6. De conformidad con el artículo 75, los Estados miembros conferirán a sus autoridades de vigilancia del mercado la facultad de exigir a los proveedores y posibles proveedores que faciliten información, de llevar a cabo inspecciones a distancia o in situ sin previo aviso y de realizar controles del desarrollo de los ensayos en condiciones reales y de los productos relacionados. Las autoridades de vigilancia del mercado utilizarán estas competencias para garantizar el desarrollo seguro de los ensayos en condiciones reales.

7. Cualquier incidente grave detectado en el transcurso de las pruebas en condiciones reales se notificará a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 73. El proveedor o posible proveedor adoptará medidas paliativas inmediatas o, en su defecto, suspenderá los ensayos en condiciones reales hasta que se lleve a cabo dicha paliación o, de lo contrario, pondrá fin a los mismos. El proveedor o posible proveedor establecerá un procedimiento para la rápida recuperación del sistema de IA tras la finalización de las pruebas en condiciones reales.

8. Los proveedores o posibles proveedores notificarán a la autoridad nacional de vigilancia del mercado del Estado miembro en el que vayan a realizarse las pruebas en condiciones reales la suspensión o finalización de las pruebas en condiciones reales y los resultados finales.

9. El proveedor o posible proveedor será responsable, en virtud de la legislación nacional y de la Unión aplicable en materia de responsabilidad civil, de cualquier daño causado en el transcurso de sus pruebas en condiciones reales.

Artículo 61

Consentimiento informado para participar en pruebas en condiciones del mundo real fuera de los espacios aislados de regulación de la IA.

1. *A efectos de las pruebas en condiciones reales contempladas en el artículo 60, se obtendrá el consentimiento informado libremente otorgado de los sujetos de las pruebas antes de su participación en las mismas y después de haber sido debidamente informados con datos concisos, claros, pertinentes y comprensibles sobre:*

   (a) la naturaleza y los objetivos de las pruebas en condiciones del mundo real y los posibles inconvenientes que pueda acarrear su participación;

   (b) las condiciones en las que se realizarán los ensayos en condiciones reales, incluida la duración prevista de la participación del sujeto o sujetos;

   (c) sus derechos y las garantías relativas a su participación, en particular su derecho a negarse a participar en los ensayos en condiciones reales y a retirarse de los mismos en cualquier momento, sin que ello suponga perjuicio alguno y sin tener que aportar justificación alguna;

(d) las modalidades para solicitar la anulación o el incumplimiento de las predicciones, recomendaciones o decisiones del sistema de IA;

(e) el número único de identificación a escala de la Unión del ensayo en condiciones reales, de conformidad con el artículo 60, apartado 4***, letra*** c***), y los datos de contacto del proveedor o de su representante legal de quien pueda obtenerse más información.***

2. El consentimiento informado se fechará y documentará y se entregará una copia a los sujetos de ensayo o a su representante legal.

Artículo 62

Medidas para ▌ *proveedores e* ***implantadores, en particular las PYME, incluidas las empresas de nueva creación.***

1. Los Estados miembros emprenderán las siguientes acciones:

(a) proporcionará a ***las PYME, incluidas las de nueva*** creación***, que tengan un domicilio social o una sucursal en la Unión,*** acceso prioritario a los entornos aislados de regulación de la IA***, en la*** medida en que cumplan las condiciones de admisibilidad y ***los criterios de selección. El acceso prioritario no impedirá que otras PYME, incluidas las de nueva creación, distintas de las mencionadas en el párrafo primero, accedan al arenero regulador de la IA, siempre que también cumplan las condiciones de admisibilidad y los criterios de selección***;

(b) organizar actividades específicas de sensibilización ***y formación sobre*** la aplicación del presente Reglamento adaptadas a las necesidades de las ***PYME, incluidas las empresas de nueva creación, los usuarios y, en su caso, las autoridades públicas locales***;

(c) ***utilizar los canales específicos existentes y***, en su caso, establecer ***otros nuevos*** para la comunicación con ***las PYME, incluidas las empresas de nueva creación, los usuarios, otros innovadores y, cuando proceda, las autoridades públicas locales,*** a fin de proporcionar ***asesoramiento*** y responder a las preguntas sobre la aplicación del presente Reglamento***, incluso en lo que se refiere a la participación en los espacios aislados de regulación de la IA;***

(d) facilitar la participación de las PYME y otras partes interesadas en el proceso de elaboración de normas.

2. Se tendrán en cuenta los intereses y necesidades específicos de ***las PYME*** proveedoras***, incluidas las de nueva creación,*** a la hora de fijar las tasas para la evaluación de la conformidad con arreglo al artículo 43, reduciendo dichas tasas proporcionalmente a su tamaño***, tamaño de mercado y otros indicadores pertinentes***.

3. La Oficina de AI emprenderá las siguientes acciones:

(a) proporcionar plantillas normalizadas para los ámbitos cubiertos por el presente Reglamento, según especifique la Junta en su solicitud motivada;

(b) desarrollar y mantener una plataforma de información única que proporcione información de fácil uso en relación con este Reglamento para todos los operadores de la Unión;

(c) organizar campañas de comunicación adecuadas para dar a conocer las obligaciones derivadas del presente Reglamento;

(d) evaluar y promover la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

Artículo 63

Excepciones para operadores específicos

1. Las microempresas, en el sentido de la Recomendación 2003/361/CE, podrán cumplir determinados elementos del sistema de gestión de la calidad exigido en el artículo 17 del presente Reglamento de forma simplificada, siempre que no tengan empresas asociadas o empresas vinculadas en el sentido de dicha Recomendación. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que podrán cumplirse de manera simplificada teniendo en cuenta las necesidades de las microempresas, sin que ello afecte al nivel de protección ni a la necesidad de cumplir los requisitos relativos a los sistemas de IA de alto riesgo.

2. El apartado 1 del ***presente artículo no se interpretará en el sentido de que exime a dichos operadores del cumplimiento de cualesquiera otros requisitos u obligaciones establecidos en el presente Reglamento, incluidos los establecidos en los artículos 9, 10, 11, 12, 13, 14, 15, 72 y 73.***

CAPÍTULO VII
GOBERNANZA

Sección 1

Gobernanza a escala de la Unión

Artículo 64
Oficina IA

1. ***La Comisión desarrollará los conocimientos y capacidades de la Unión en el ámbito de la IA a través de la Oficina de IA.***

2. ***Los Estados miembros facilitarán las tareas encomendadas a la Oficina de AI, tal y como se refleja en el presente Reglamento.***

Artículo 65

Creación y estructura del Consejo Europeo de Inteligencia Artificial

1. Se crea una Junta Europea de Inteligencia Artificial (la "Junta").

2. El Consejo estará compuesto por un representante de cada Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de AI también asistirá a las reuniones del Consejo, sin participar en las votaciones. La Junta podrá invitar a las reuniones, caso por caso, a otras autoridades, organismos o expertos nacionales y de la Unión, cuando las cuestiones debatidas sean pertinentes para ellos.

3. Cada representante será designado por su Estado miembro por un período de tres años, renovable una sola vez.

4. Los Estados miembros velarán por que sus representantes en el Consejo:

(a) dispongan de las competencias y poderes pertinentes en su Estado miembro para contribuir activamente a la realización de las tareas del Consejo contempladas en el artículo 66;

(b) se designan como punto de contacto único ante el Consejo y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

(c) están facultados para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes de su Estado miembro en lo que respecta a la aplicación del presente Reglamento, incluso mediante la recopilación de datos e información pertinentes para el cumplimiento de sus funciones en el Consejo.

5. Los representantes designados de los Estados miembros aprobarán el reglamento interno del Consejo por mayoría de dos tercios. El reglamento interno establecerá, en particular, las modalidades del proceso de selección, la duración del mandato del Presidente y la especificación de sus funciones, las modalidades de votación y la organización de las actividades del Consejo y de sus subgrupos.

6. El Consejo creará dos subgrupos permanentes para proporcionar una plataforma para la cooperación y el intercambio entre las autoridades de vigilancia del mercado y para notificar a las autoridades cuestiones relacionadas con la vigilancia del mercado y los organismos notificados.

El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

El Consejo podrá crear otros subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas. Cuando proceda, podrá invitarse a representantes del foro consultivo contemplado en el artículo 67 a dichos subgrupos o a reuniones específicas de los mismos en calidad de observadores.

7. ***El Consejo se organizará y funcionará de forma que se salvaguarde la objetividad e imparcialidad de sus actividades.***

8. ***La Junta estará presidida por uno de los representantes de los Estados miembros. La Oficina de AI se encargará de la secretaría de la Junta. Convocará las reuniones a petición del Presidente y preparará el orden del día de conformidad con las tareas de la Junta con arreglo al presente Reglamento y a su reglamento interno.***

Artículo 66

Funciones del Consejo

La Junta asesorará y asistirá a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, la Junta ***podrá***, en particular:

(a) ***contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación con las autoridades de vigilancia del mercado afectadas y previo acuerdo de las mismas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo*** 74, apartado 11;

(b) ***recopilar y compartir conocimientos técnicos y*** reglamentarios ***y buenas prácticas entre los Estados miembros***;

(c) asesorar sobre la aplicación del presente Reglamento, en particular por lo que se refiere a la aplicación de las normas relativas a los modelos de IA de propósito general;

(d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, incluso en relación con la excepción a los procedimientos de evaluación de la conformidad a que se refiere el artículo 46, el funcionamiento de los "cajones de arena" reglamentarios y los ensayos en condiciones reales a que se refieren los artículos 57, 59 y 60;

(e) a petición de la Comisión o por iniciativa propia, emitir recomendaciones ***y dictámenes*** escritos ***sobre cualquier*** asunto ***pertinente*** relacionado con la ejecución del presente Reglamento ***y con su aplicación coherente y eficaz, incluyendo:***

(i) sobre la elaboración y aplicación de códigos de conducta y códigos de prácticas con arreglo al presente Reglamento, así como de las directrices de la Comisión;

(ii) la evaluación y revisión del presente Reglamento de conformidad con el artículo 112, incluido lo relativo a los informes sobre incidentes graves a que se refiere el artículo 73, y el funcionamiento de la base de datos a que se refiere el artículo 71, la preparación de los actos delegados o de ejecución, y lo relativo a las posibles adaptaciones del presente Reglamento a los actos jurídicos enumerados en el anexo I;

(iii) sobre las especificaciones técnicas o las normas existentes en relación con los requisitos establecidos en la sección 2 del capítulo III;

(iv) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41;

(v) tendencias, como la competitividad global europea en IA, la adopción de la IA en la Unión y el desarrollo de competencias digitales;

(vi) tendencias sobre la ***evolución de la tipología de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de responsabilidad;***

(vii) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7, y sobre la posible necesidad de revisar el artículo 5 de conformidad con el artículo 112, teniendo en cuenta las pruebas pertinentes disponibles y los últimos avances tecnológicos;

(f) apoyar a la Comisión en la promoción de la alfabetización en IA, la concienciación pública y la comprensión de los beneficios, riesgos, salvaguardias y derechos y obligaciones en relación con el uso de los sistemas de IA;

(g) facilitar el desarrollo de criterios comunes y una comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, incluso contribuyendo al desarrollo de índices de referencia;

(h) cooperar, según proceda, con otras instituciones, órganos y organismos de la Unión, así como con los grupos y redes de expertos pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores, los datos y la protección de los derechos fundamentales;

(i) contribuir a una cooperación eficaz con las autoridades competentes de terceros países y con las organizaciones internacionales;

(j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos organizativos y técnicos necesarios para la aplicación del presente Reglamento, incluso contribuyendo a la evaluación de las necesidades de formación del personal de los Estados miembros que participe en la aplicación del presente Reglamento;

(k) ayudar a la Oficina de la IA a respaldar a las autoridades nacionales competentes en el establecimiento y desarrollo de los compartimentos estancos de regulación, y facilitar la cooperación y el intercambio de información entre los compartimentos estancos de regulación;

(l) contribuir a la elaboración de documentos de orientación y prestar el asesoramiento pertinente;

(m) asesorar a la Comisión en asuntos internacionales relacionados con la IA;

(n) proporcionar dictámenes a la Comisión sobre las descripciones cualificadas relativas a los modelos de IA de uso general;

(o) recibir los dictámenes de los Estados miembros sobre las descripciones cualificadas relativas a los modelos de IA de propósito general, y sobre las experiencias y prácticas nacionales en materia de vigilancia y aplicación de los sistemas de IA, en particular de los sistemas que integran los modelos de IA de propósito general.

Artículo 67 Foro consultivo

1. Se creará un foro consultivo para aportar conocimientos técnicos y asesorar al Consejo y a la Comisión, así como para contribuir a las tareas que les incumben en virtud del presente Reglamento.

2. La composición del foro consultivo representará una selección equilibrada de partes interesadas, incluidos la industria, las nuevas empresas, las PYME, la sociedad civil y el mundo académico. La composición del foro consultivo será equilibrada con respecto a los intereses comerciales y no comerciales y, dentro de la categoría de intereses comerciales, con respecto a las PYME y otras empresas.

3. La Comisión nombrará a los miembros del foro consultivo, de conformidad con los criterios establecidos en el apartado 2, de entre las partes interesadas con experiencia reconocida en el ámbito de la IA.

4. La duración del mandato de los miembros del foro consultivo será de dos años, prorrogable hasta un máximo de cuatro años.

5. La Agencia de los Derechos Fundamentales, ENISA, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI) serán miembros permanentes del foro consultivo.

6. El Foro consultivo establecerá su reglamento interno. Elegirá a dos copresidentes entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una vez. El mandato de los copresidentes será de dos años, renovable una sola vez.

7. El foro consultivo celebrará reuniones al menos dos veces al año. El foro consultivo podrá invitar a sus reuniones a expertos y otras partes interesadas.

8. El foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones escritas a petición del Consejo o de la Comisión.

9. El Foro Consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.

10. El foro consultivo elaborará un informe anual sobre sus actividades. Dicho informe se pondrá a disposición del público.

Artículo 68

Comité científico de expertos independientes

1. *La Comisión adoptará, mediante un acto de ejecución, disposiciones relativas a la creación de un grupo científico de expertos independientes (el "grupo científico") destinado a apoyar las actividades de ejecución en virtud del presente Reglamento. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.*

2. *El comité científico estará compuesto por expertos seleccionados por la Comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA necesarios para las tareas establecidas en el apartado 3, y deberán poder demostrar que cumplen todas las condiciones siguientes:*

   (a) *con conocimientos y competencias especiales y experiencia científica o técnica en el ámbito de la IA;*

(b) independencia de cualquier proveedor de sistemas de IA o de modelos o sistemas de IA de uso general;

(c) capacidad para llevar a cabo sus actividades con diligencia, precisión y objetividad. La Comisión, en consulta con el Consejo, determinará el número de expertos del panel en función de las necesidades requeridas y garantizará una representación geográfica y de género equitativa.

3. El panel científico asesorará y apoyará a la Oficina de AI, en particular en lo que respecta a las siguientes tareas:

(a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los modelos y sistemas de IA de propósito general, en particular

(i) alertar a la Oficina de la IA de posibles riesgos sistémicos a nivel de la Unión de modelos de IA de propósito general, de conformidad con el artículo 90;

(ii) Contribuir al desarrollo de herramientas y metodologías para evaluar las capacidades de los modelos y sistemas de IA de propósito general, entre otras cosas mediante evaluaciones comparativas;

(iii) asesorar sobre la clasificación de los modelos de IA de uso general con riesgo sistémico;

(iv) asesorar sobre la clasificación de diversos modelos y sistemas de IA de uso general;

(v) contribuir al desarrollo de herramientas y plantillas;

(b) apoyar la labor de las autoridades de vigilancia del mercado, a petición de éstas;

(c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el Artículo 74, apartado 11***, sin perjuicio de las competencias de las autoridades de vigilancia del mercado;***

(d) apoyar a la Oficina de AI en el desempeño de sus funciones en el contexto de la cláusula de salvaguardia de conformidad con el artículo 81.

4. 3. Los expertos del Comité científico desempeñarán sus tareas con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el desempeño de sus tareas y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones con arreglo al apartado 3. Cada experto elaborará una declaración de intereses, que se hará pública. La Oficina de AI establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, los procedimientos y las modalidades para que la comisión técnica científica y sus miembros emitan descripciones y soliciten la asistencia de la Oficina de la IA para la realización de las tareas de la comisión técnica científica.

Artículo 69

Acceso de los Estados miembros a la reserva de expertos

1. *Los Estados miembros podrán recurrir a los expertos de la comisión técnica científica para que les apoyen en sus actividades de aplicación del presente Reglamento.*

2. *Podrá exigirse a los Estados miembros el pago de tasas por el asesoramiento y la asistencia prestados por los expertos. La estructura y el nivel de las tasas, así como la escala y la estructura de los costes recuperables se establecerán en el acto de ejecución a que se refiere el artículo 68, apartado 1, teniendo en cuenta los objetivos de la aplicación adecuada del presente Reglamento, la rentabilidad y la necesidad de garantizar el acceso efectivo de todos los Estados miembros a los expertos.*

3. *La Comisión facilitará el acceso oportuno a los expertos por parte de los Estados miembros, según sea necesario, y garantizará que la combinación de las actividades de apoyo llevadas a cabo por la IA de la Unión en apoyo de las pruebas con arreglo al artículo* 84 *y los expertos con arreglo al presente artículo se organice de manera eficiente y aporte el mejor valor añadido posible.*

Sección 2

Autoridades nacionales competentes

Artículo 70

Designación de autoridades nacionales competentes ***y ventanilla única***

1. Cada Estado miembro ***establecerá o*** designará ***como*** autoridades nacionales competentes al ***menos una autoridad notificante y una*** autoridad de ***vigilancia del mercado a efectos del presente Reglamento***. ***Dichas autoridades*** nacionales ***competentes ejercerán sus competencias con independencia, imparcialidad y neutralidad, a fin de salvaguardar la objetividad de sus actividades y funciones y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de dichas autoridades se abstendrán de toda acción incompatible con sus funciones. Siempre que se respeten estos principios, dichas actividades y tareas podrán ser realizadas por una o varias autoridades designadas, en función de las necesidades organizativas del Estado miembro***.

2. Los Estados miembros ***comunicarán a*** la Comisión la ***identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público información sobre la manera de ponerse en contacto con las autoridades competentes y las ventanillas únicas***, ***a través de medios de comunicación electrónica, a más tardar el ... [12 meses a partir de la fecha de entrada en vigor del presente Reglamento]. Los Estados miembros designarán a una autoridad de vigilancia del mercado para que actúe como punto de contacto único para el presente Reglamento, y notificarán a la Comisión la identidad del punto de contacto único. La Comisión pondrá a disposición del público una lista de los puntos de contacto únicos***.

3. Los Estados miembros velarán por que ***sus autoridades nacionales competentes dispongan de*** los recursos ***técnicos,*** financieros y humanos adecuados***, así como de la infraestructura*** necesaria para desempeñar ***eficazmente*** sus funciones con arreglo al presente Reglamento. En particular, ***las autoridades nacionales*** competentes dispondrán permanentemente de un número suficiente de personal cuyas competencias y conocimientos especializados incluirán una comprensión profunda de las tecnologías de la IA, los datos y la informática de datos, la ***protección de datos personales, la ciberseguridad, los*** derechos fundamentales, los riesgos para la salud y la seguridad y el conocimiento de las normas y requisitos jurídicos existentes. ***Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.***

4. Las autoridades nacionales competentes adoptarán un nivel adecuado de medidas de ciberseguridad.

5. En el ejercicio de sus funciones, las autoridades nacionales competentes actuarán respetando las obligaciones de confidencialidad establecidas en el artículo 78.

6. ***A más tardar el ...,*** [***un año después de la fecha de entrada en vigor del presente Reglamento***] ***y, posteriormente, una vez cada dos años, los*** Estados miembros informarán a la Comisión ▌ sobre la situación de los recursos financieros y humanos de las autoridades nacionales competentes, con una evaluación de su adecuación. La Comisión transmitirá esa información a la Junta para su debate y posibles recomendaciones.

7. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.

8. Las autoridades nacionales competentes podrán proporcionar orientación y asesoramiento sobre la aplicación del presente Reglamento, ***en particular a las PYME, incluidas las de nueva creación, teniendo en cuenta la orientación y el asesoramiento de la Junta y de la Comisión, según proceda***. Cuando las autoridades nacionales competentes tengan la intención de proporcionar orientación y asesoramiento con respecto a un sistema de IA en ámbitos cubiertos por otra legislación de la Unión, se consultará a las autoridades nacionales competentes en virtud de dicha legislación de la Unión, según proceda. ▌

9. Cuando las instituciones, órganos u organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como autoridad competente para su supervisión.

CAPÍTULO VIII

BASE DE DATOS DE LA UE PARA ▌ SISTEMAS DE AI DE ALTO RIESGO

Artículo 71

Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el anexo III

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contenga la información a que se refieren ***los apartados 2 y 3 del presente artículo sobre los*** sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados de conformidad con ***los artículos 49 y 60. Al establecer las especificaciones funcionales de dicha base de datos, la Comisión consultará a los expertos pertinentes, y al actualizar las especificaciones funcionales de dicha base de datos, la Comisión consultará al Consejo***.

2. Los datos enumerados en la ***sección A del*** anexo VIII serán introducidos en la base de datos de la UE por el ***proveedor o, en su caso, por el representante autorizado***.

3. Los datos enumerados en la sección C del anexo VIII serán introducidos en la base de datos de la UE por el responsable del despliegue que sea una autoridad, agencia u organismo público, o que actúe en su nombre, de conformidad con los apartados 2 y 3 del artículo 49.

4. ***Con excepción de la sección contemplada en el artículo 49, apartado 4, y en el artículo 60, apartado 5, la información*** contenida en la base de datos de la UE ***registrada de conformidad con el artículo 49*** deberá ***ser*** accesible ***y estar a disposición del público de forma fácil de utilizar. La información deberá ser fácilmente navegable y legible por máquina. La información registrada de conformidad con el artículo 60 sólo será accesible a las autoridades de vigilancia del mercado y a la Comisión, a menos que el proveedor o prestador potencial haya dado su consentimiento para que la información sea también accesible al*** público.

5. La base de datos de la UE sólo contendrá datos personales en la medida en que sea necesario para recoger y tratar información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro del sistema y con autoridad legal para representar al proveedor ***o al implantador, según proceda***.

6. La Comisión será el controlador de la base de datos de la UE. Pondrá a ***disposición de los proveedores, posibles*** proveedores ***e implantadores*** un apoyo técnico y administrativo adecuado. ***La base de datos de la UE cumplirá los requisitos de accesibilidad aplicables.***

CAPÍTULO IX
SEGUIMIENTO POSTCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN, VIGILANCIA DEL MERCADO

Sección 1
Seguimiento postcomercialización

Artículo 72

Seguimiento postcomercialización por parte de los proveedores y plan de seguimiento postcomercialización para los sistemas de IA de alto riesgo

1. Los proveedores establecerán y documentarán un sistema de seguimiento postcomercialización de manera proporcionada a la naturaleza de las tecnologías de IA y a los riesgos del sistema de IA de alto riesgo.

2. El sistema de seguimiento poscomercialización recopilará, documentará y analizará de forma activa y sistemática los datos pertinentes que ***puedan*** facilitar ***los implantadores o que puedan*** recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo a lo largo de su vida útil, y que permitan al proveedor evaluar la conformidad continua de los sistemas de IA con los requisitos establecidos en el capítulo III, sección 2. ***Cuando proceda, la supervisión posterior a la comercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no cubrirá los datos operativos sensibles de los implantadores que sean autoridades policiales.***

3. El sistema de seguimiento poscomercialización se basará en un plan de seguimiento poscomercialización. El plan de seguimiento poscomercialización formará parte de la documentación técnica a que se refiere el Anexo IV. La Comisión adoptará un acto de ejecución por el que se establezcan disposiciones detalladas que determinen un modelo para el plan de seguimiento poscomercialización y la lista de elementos que deben incluirse en el plan ***a más tardar ... [seis meses antes de la entrada en aplicación del presente Reglamento]***. ***Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.***

4. En el caso de los sistemas de IA de alto riesgo cubiertos por la legislación de armonización de la Unión enumerada en ***la sección A del*** anexo I, cuando ya se hayan establecido un sistema y un plan de seguimiento poscomercialización con arreglo a dicha legislación, a ***fin de garantizar la coherencia, evitar duplicaciones y minimizar las cargas adicionales, los proveedores tendrán la opción de integrar, según proceda, los*** elementos ***necesarios*** descritos en los apartados 1, 2 y 3 ***utilizando la plantilla a que se refiere el apartado 3 en*** los sistemas y planes ya existentes ***con arreglo a dicha legislación, siempre que con ello se consiga un nivel de protección equivalente***.

   El párrafo primero del presente apartado también se aplicará ▌ a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto ***5***, comercializados o puestos en servicio por entidades ***financieras que estén sujetas a requisitos en virtud de la legislación de la Unión en materia de servicios financieros en relación con su gobernanza, disposiciones o procesos internos***.

Sección 2

Intercambio de información sobre incidentes graves

Artículo 73

Notificación de incidentes graves

1. Los proveedores de sistemas de IA de alto riesgo comercializados en el mercado de la Unión informarán de cualquier incidente grave ***a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente.***

.

2. ***El*** informe a ***que se refiere el apartado*** 1 se efectuará inmediatamente después de que el proveedor haya establecido un nexo causal entre el sistema de IA y el incidente ***grave*** o ▌ la probabilidad razonable de que exista tal nexo y, en cualquier caso, a más tardar 15 días después de que el ***proveedor o, en su caso, el implantador, tenga*** conocimiento del incidente grave***.***

El plazo de notificación a que se refiere el párrafo primero tendrá en cuenta la ***gravedad del*** incidente grave ▌ .

3. ***No obstante lo dispuesto en el apartado 2 del presente artículo, en caso de infracción generalizada o de incidente grave, tal como se definen en la letra b) del punto 44 del artículo 3, el informe a que se refiere el apartado 1 del presente artículo se facilitará inmediatamente, y a más tardar dos días después de que el proveedor o, en su caso, el encargado del despliegue tenga conocimiento de dicho incidente.***

5. ***3. No obstante lo dispuesto en el apartado 2, en caso de fallecimiento de una persona, el informe se facilitará inmediatamente después de que el proveedor o el encargado del despliegue haya establecido, o tan pronto como lo sospeche, una relación causal entre el sistema de IA de alto riesgo y el incidente grave, pero a más tardar diez días después de la fecha en que el proveedor o, en su caso, el encargado del despliegue tenga conocimiento del incidente grave.***

6. ***Cuando sea necesario para garantizar la puntualidad de los informes, el proveedor o, en su caso, el encargado del despliegue, podrá presentar un informe inicial incompleto, seguido de un informe completo***.

7. ***Tras la notificación de un incidente grave con arreglo al apartado 1, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación del riesgo del incidente y medidas correctoras.***

   El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado de que se trate, durante las investigaciones a que se refiere el párrafo primero, y no llevará a cabo ninguna investigación que implique la alteración del sistema de IA de que se trate de forma que pueda afectar a cualquier evaluación posterior de las causas del incidente, antes de informar de dicha acción a las autoridades competentes.

8. Al recibir una notificación relativa a un ***incidente grave contemplado en el artículo 3, punto 44, letra c), la*** autoridad de vigilancia del mercado ***pertinente*** informará a las autoridades u organismos públicos nacionales contemplados en el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el ... [12 meses después de la entrada en vigor del presente Reglamento]***, y se evaluarán periódicamente***.

9. La autoridad de vigilancia del mercado adoptará las medidas adecuadas, conforme a lo dispuesto en el artículo 19 del Reglamento (UE) 2019/1020, en un plazo de siete días a partir de la fecha en que haya recibido la notificación a que se refiere el apartado 1 del presente artículo, y seguirá los procedimientos de notificación previstos en dicho Reglamento.

10. En el caso de los sistemas de IA de alto riesgo mencionados en el ▌ anexo III ***que*** sean comercializados o puestos en servicio por proveedores ***sujetos a instrumentos legislativos de la Unión que establezcan obligaciones de notificación equivalentes a las establecidas en el presente*** Reglamento ▌, la notificación de incidentes graves se limitará a los contemplados ***en el artículo 3, punto 44, letra c)***.

11. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos, o sean ellos mismos productos, cubiertos por los Reglamentos (UE) 2017/745 y (UE) 2017/746, la notificación de incidentes graves se limitará a los contemplados en el artículo 3, punto 44, letra c), del presente Reglamento, y se efectuará a la autoridad nacional competente elegida a tal efecto por los Estados miembros en los que se haya producido el incidente.

12. Las autoridades nacionales competentes notificarán inmediatamente a la Comisión cualquier incidente grave, hayan tomado o no medidas al respecto, de conformidad con el artículo 20 del Reglamento (UE) 2019/1020.

Sección 3

Ejecución

Artículo 74

Vigilancia del mercado y control de los sistemas de IA en el mercado de la Unión

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA cubiertos por el presente Reglamento. A efectos de la aplicación efectiva del presente Reglamento:

   (a) cualquier referencia a un operador económico en virtud del Reglamento (UE) 2019/1020 se entenderá que incluye a todos los operadores identificados en ***el artículo 2, apartado 1,*** del presente Reglamento;

   (b) cualquier referencia a un producto con arreglo al Reglamento (UE) 2019/1020 se entenderá que incluye todos los sistemas de IA incluidos en el ámbito de aplicación del presente Reglamento.

2. ***Como parte de sus obligaciones de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de*** vigilancia del mercado comunicarán ***anualmente*** a la Comisión y a las autoridades nacionales de competencia pertinentes cualquier información identificada en el curso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. ***También informarán anualmente a la Comisión sobre el uso de prácticas prohibidas que se haya producido durante ese año y sobre las medidas adoptadas.***

3. 2. Para los sistemas de IA de alto riesgo relacionados con productos cubiertos por la legislación de armonización de la Unión enumerada en la sección A del anexo I, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos jurídicos. 3. ***No obstante lo dispuesto en el apartado 2, y en circunstancias apropiadas, los Estados miembros podrán designar a otra autoridad pertinente para que actúe como autoridad de vigilancia del mercado, siempre que garanticen la coordinación con las autoridades sectoriales pertinentes de vigilancia del mercado responsables de la aplicación de los actos jurídicos enumerados en el anexo I.***

4. Los procedimientos contemplados en los artículos 79 a 83 del presente Reglamento no se aplicarán a los sistemas de IA relacionados con los productos cubiertos por la legislación de armonización de la Unión enumerada en la sección A del anexo I, cuando dichos actos jurídicos ya prevean procedimientos que garanticen un nivel de protección equivalente y tengan el mismo objetivo. En tales casos, se aplicarán en su lugar los procedimientos sectoriales pertinentes.

5. ***Sin perjuicio de las competencias de las autoridades de vigilancia del mercado con arreglo al artículo 14 del Reglamento (UE) 2019/1020, a fin de garantizar la aplicación efectiva del presente Reglamento, las autoridades de vigilancia del mercado podrán ejercer las competencias a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento de forma remota, según proceda.***

6. Por lo que respecta a los sistemas de IA ***de alto riesgo comercializados***, puestos en servicio o utilizados por entidades financieras reguladas por la legislación de la Unión en materia de servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad ***nacional*** pertinente responsable de la supervisión financiera de dichas entidades con arreglo a dicha legislación ***en la medida en que la comercialización, puesta en servicio o utilización del sistema de IA guarde relación directa con la prestación de dichos servicios financieros***.

7. ***No obstante lo dispuesto en el apartado 6, en circunstancias apropiadas, y siempre que se garantice la coordinación, el Estado miembro podrá designar a otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.***

Las autoridades nacionales de vigilancia del mercado que supervisen entidades de crédito reguladas con arreglo a la Directiva 2013/36/UE, que participen en el Mecanismo Único de Supervisión establecido por el Reglamento n.º 1024/2013, deben comunicar sin demora al Banco Central Europeo toda información detectada en el curso de sus actividades de vigilancia del mercado que pueda ser de interés potencial para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

8. Para los sistemas de IA ***de alto riesgo enumerados*** en el punto 1 del anexo III, en la medida en que los sistemas se utilicen con fines policiales, de gestión de fronteras y de justicia y democracia, ***y para los sistemas de IA de alto riesgo enumerados en*** los puntos 6***, 7 y 8*** del anexo III del presente Reglamento, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control competentes en materia de protección de datos en virtud ***del Reglamento (UE) 2016/679 o de*** la Directiva (UE) 2016/680, ***bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en*** los artículos 41 a 44 ***de la*** Directiva ***(UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales, ni interferirán de otro modo en sus actividades cuando actúen en el ejercicio de sus funciones jurisdiccionales.***

9. Cuando las instituciones, órganos u organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como su autoridad de vigilancia del mercado, ***excepto en relación con el Tribunal de Justicia de la Unión Europea cuando actúe en ejercicio de sus funciones jurisdiccionales***.

10. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas en virtud del presente Reglamento y otras autoridades u organismos nacionales pertinentes que supervisen la aplicación de la legislación de armonización de la Unión enumerada en el anexo I, o en otra legislación de la Unión, que pueda ser pertinente para los sistemas de IA de alto riesgo mencionados en el anexo III.

11. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que llevarán a cabo las autoridades de vigilancia del mercado o las autoridades de vigilancia del mercado conjuntamente con la Comisión, que tengan por objeto promover el cumplimiento, identificar el incumplimiento, aumentar la sensibilización o proporcionar orientación en relación con el presente Reglamento con respecto a categorías específicas de sistemas de IA de alto riesgo que se considere que presentan un riesgo grave en dos o más Estados miembros de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de Inteligencia Artificial prestará apoyo a la coordinación de las investigaciones conjuntas.

12. Sin perjuicio de las competencias previstas en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de formación, validación y ensayo utilizados para el desarrollo de sistemas de IA de alto riesgo, incluso, cuando proceda y con sujeción a las salvaguardias de seguridad, a través de interfaces de programación de aplicaciones ("API") u otros medios técnicos y herramientas pertinentes que permitan el acceso a distancia.

13. Las autoridades de vigilancia del mercado tendrán acceso al código fuente del sistema de IA de alto riesgo previa solicitud motivada y sólo cuando se cumplan las dos condiciones siguientes:

(a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 del capítulo III; y

(b) se hayan agotado o resultado insuficientes los procedimientos de prueba o auditoría y las comprobaciones basadas en los datos y la documentación facilitados por el proveedor.

14. Toda información o documentación obtenida por las autoridades de vigilancia del mercado se tratará respetando las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 75

Asistencia mutua, vigilancia del mercado y control de los sistemas de IA de uso general

1. Cuando un sistema de IA se base en un modelo de IA de propósito general, y el modelo y el sistema sean desarrollados por el mismo proveedor, la Oficina de IA tendrá competencias para vigilar y supervisar el cumplimiento por dicho sistema de IA de las obligaciones derivadas del presente Reglamento. Para llevar a cabo sus tareas de seguimiento y supervisión, la Oficina de IA tendrá todas las competencias de una autoridad de vigilancia del mercado en el sentido del Reglamento (UE) 2019/1020.

2. Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de propósito general que puedan ser utilizados directamente por los implantadores para al menos un fin clasificado como de alto riesgo con arreglo al presente Reglamento incumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento e informarán de ello al Consejo y a las demás autoridades de vigilancia del mercado.

3. Cuando una autoridad nacional de vigilancia del mercado no pueda concluir su investigación del sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA a pesar de haber realizado todos los esfuerzos adecuados para obtener dicha información, podrá presentar una solicitud motivada a la Oficina de IA, mediante la cual se hará efectivo el acceso a dicha información. En ese caso, la Oficina de IA facilitará a la autoridad solicitante sin demora, y en cualquier caso en un plazo de 30 días, cualquier información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades nacionales del mercado salvaguardarán la confidencialidad de la información que obtengan de conformidad con el artículo 78 del presente Reglamento. Se aplicará mutatis mutandis el procedimiento previsto en el capítulo VI del Reglamento (UE) 2019/1020.

Artículo 76

Supervisión de las pruebas en condiciones reales por parte de las autoridades de vigilancia del mercado

1. ***Las autoridades de vigilancia del mercado tendrán competencias y facultades para garantizar que los ensayos en condiciones reales sean conformes al presente Reglamento.***

2. ***Cuando se realicen ensayos en condiciones reales para sistemas de IA supervisados dentro de un recinto de seguridad regulatorio de la IA con arreglo al artículo 59, las autoridades de vigilancia del mercado verificarán el cumplimiento de las disposiciones del artículo 60 como parte de su función de supervisión del recinto de seguridad regulatorio de la IA. Dichas autoridades podrán, en su caso, permitir que las pruebas en condiciones reales sean realizadas por el proveedor o posible proveedor, como excepción a las condiciones establecidas en el artículo 60, apartado 4, letras f) y g).***

3. ***Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o cualquier tercero de un incidente grave o tenga otros motivos para considerar que no se cumplen las condiciones establecidas en los artículos 60 y 61, podrá adoptar en su territorio, según proceda, cualquiera de las siguientes decisiones:***

   (a) suspender o finalizar las pruebas en condiciones reales;

(b) exigir al proveedor o posible proveedor y a los usuarios que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión de las contempladas en el apartado 3 del presente artículo, o haya formulado una objeción en el sentido del artículo 60, apartado 4, letra b), la decisión o la objeción indicarán los motivos de la misma y la forma en que el proveedor o posible proveedor puede impugnar la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión de las contempladas en el apartado 3, comunicará los motivos de la misma a las autoridades de vigilancia del mercado de otros Estados miembros en los que se haya sometido a ensayo el sistema de IA de conformidad con el plan de ensayo.

Artículo 77

Competencias de las autoridades de protección de los derechos fundamentales

1. Las autoridades u organismos públicos nacionales que supervisen o hagan cumplir las obligaciones derivadas del Derecho de la Unión que protegen los derechos fundamentales***, incluido el derecho a la no discriminación,*** en relación con el uso de los sistemas de IA de alto riesgo a que se refiere el anexo III estarán facultados para solicitar y acceder a cualquier documentación creada o conservada ***en*** virtud del presente Reglamento ***en una lengua y formato accesibles*** cuando el acceso a dicha documentación sea necesario para el ***cumplimiento efectivo de*** sus mandatos dentro de los límites de su jurisdicción. La autoridad u organismo público pertinente informará de dicha solicitud a la autoridad de vigilancia del mercado del Estado miembro de que se trate.

2. A más tardar el ... [***tres*** meses después de la entrada en vigor del presente Reglamento], cada Estado miembro identificará a las autoridades u organismos públicos a que se refiere el apartado 1 y pondrá a disposición del público una lista de los mismos ▌ . Los Estados miembros notificarán la lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

3. Cuando la documentación a que se refiere el apartado 1 sea insuficiente para determinar si se ha producido una infracción de las obligaciones derivadas del Derecho de la Unión que protegen los derechos fundamentales, la autoridad u organismo público a que se ***refiere*** el apartado 1 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para que organice la comprobación del sistema de IA de alto riesgo por medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha participación de la autoridad u organismo público solicitante en un plazo razonable a partir de la solicitud.

4. Toda información o documentación obtenida por las autoridades u organismos públicos nacionales a que se refiere el apartado 1 del presente artículo en virtud del presente artículo se tratará respetando las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 78

Confidencialidad

1. ***La Comisión, las*** autoridades de ***vigilancia del mercado*** y los organismos notificados***, así como cualquier otra persona física o jurídica*** implicada en la aplicación del presente Reglamento, respetarán***, de conformidad con el Derecho de la Unión y nacional,*** la confidencialidad de la información y los datos obtenidos en el desempeño de sus funciones y actividades, de manera que se proteja, en particular***:***

   (a) los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del **Consejo60** relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas***;***

---

60 Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas

(DO L 157 de 15.6.2016, p. 1).

(b) la aplicación efectiva del presente Reglamento, en particular a efectos de inspecciones, investigaciones o auditorías; ▌

(c) intereses públicos y de seguridad nacional;

(d) el desarrollo de procedimientos penales o administrativos;

(e) información clasificada con arreglo al Derecho de la Unión o nacional.

2. Las autoridades que participen en la aplicación del presente Reglamento con arreglo al apartado 1 solicitarán únicamente los datos que sean estrictamente necesarios para la evaluación del riesgo que plantean los sistemas de IA y para el ejercicio de sus competencias en cumplimiento del presente Reglamento y del Reglamento (UE) 2019/1020. Establecerán medidas de ciberseguridad adecuadas y eficaces para proteger la seguridad y confidencialidad de la información y los datos obtenidos, y suprimirán los datos recabados tan pronto como ya no sean necesarios para los fines para los que se obtuvieron, de conformidad con el Derecho de la Unión o nacional aplicable.

3. Sin perjuicio de lo dispuesto en los apartados 1 ***y 2,*** la información intercambiada con carácter confidencial entre las autoridades nacionales competentes o entre las autoridades nacionales competentes y la Comisión no se divulgará sin consulta previa a la autoridad nacional competente de origen y al ***responsable del despliegue*** cuando los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 o 7 del anexo III sean utilizados por las autoridades policiales, de control fronterizo***, de inmigración*** o de asilo y cuando dicha divulgación pudiera poner en peligro los intereses de la seguridad pública y nacional. ***Este intercambio de información no abarcará los datos operativos sensibles en relación con las actividades de las autoridades policiales, de control fronterizo, de inmigración o de asilo.***

Cuando las autoridades policiales, de inmigración o de asilo sean los proveedores de los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 o 7 del anexo III, la documentación técnica a que se refiere el anexo IV permanecerá en los locales de dichas autoridades. Dichas autoridades velarán por que las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartados 8 y 9, según proceda, puedan, previa solicitud, acceder inmediatamente a la documentación u obtener una copia de la misma. Únicamente el personal de la autoridad de vigilancia del mercado que posea el nivel adecuado de habilitación de seguridad podrá acceder a dicha documentación o a cualquier copia de la misma.

4. Los apartados 1, ***2*** y 3 no afectarán a los derechos y obligaciones de la Comisión, los Estados miembros y ***sus autoridades competentes, así como a los de los*** organismos notificados***,*** en materia de intercambio de información y difusión de alertas, ***incluso en el contexto de la cooperación transfronteriza,*** ni a las obligaciones de las partes interesadas de facilitar información con arreglo al Derecho penal de los Estados miembros.

5. La Comisión y los Estados miembros podrán intercambiar, en caso necesario ***y de conformidad con las disposiciones pertinentes de los acuerdos internacionales y comerciales***, información confidencial con las autoridades reguladoras de terceros países con las que hayan celebrado acuerdos bilaterales o multilaterales de confidencialidad que garanticen un nivel adecuado de confidencialidad.

Artículo 79

Procedimiento nacional para tratar los sistemas de IA que presentan un riesgo

1. Los sistemas de IA que presenten un riesgo se entenderán como un "producto que presenta un riesgo", tal como se define en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riesgos para la salud o la seguridad, o para ▌ los derechos fundamentales de las personas.

2. 2. Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo de los contemplados en el apartado 1 del presente artículo, llevará ***a cabo*** una evaluación del sistema de IA en cuestión con respecto a su conformidad con todos los requisitos y obligaciones establecidos en el presente Reglamento. ***Se prestará especial atención a los sistemas de IA que presenten un riesgo para los grupos de personas vulnerables a que se refiere el artículo 5. Cuando se detecten riesgos para*** los derechos fundamentales de las personas, la autoridad de vigilancia del mercado también informará a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, ***y cooperará plenamente con ellos***. Los agentes económicos pertinentes cooperarán en la medida de lo necesario con ***la autoridad de vigilancia del mercado*** y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1**.**

Cuando, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado o, ***en su caso, la*** autoridad de vigilancia del mercado ***en cooperación con la autoridad pública nacional a que se refiere el artículo 77, apartado 1,*** constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al agente económico pertinente que adopte todas las medidas correctoras adecuadas para que el sistema de IA sea conforme, que lo retire del mercado o que lo recupere en un ***plazo que*** la autoridad de vigilancia del mercado ***podrá fijar y, en cualquier caso, en el plazo más breve de quince días laborables, o en el plazo que establezca la legislación de armonización de la Unión pertinente.***

La autoridad de vigilancia del mercado informará de ello al organismo notificado pertinente. El artículo 18 del Reglamento (UE) 2019/1020 se aplicará a las medidas contempladas en el párrafo segundo del presente apartado.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará ***sin demora indebida*** a la Comisión y a los demás Estados miembros de los resultados de la evaluación y de las medidas que haya exigido adoptar al agente económico.

4. El operador velará por que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión.

5. Cuando el operador de un sistema de IA no adopte las medidas correctoras adecuadas en el plazo mencionado en el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales apropiadas para prohibir o restringir la comercialización ***o puesta en servicio*** del sistema de IA en su mercado nacional, retirar el producto ***o el sistema de IA autónomo*** de dicho mercado o recuperarlo. Dicha autoridad ***notificará sin demora indebida*** dichas medidas a la Comisión y a los demás Estados miembros ▌.

6. La ***notificación a que*** se refiere el apartado 5 incluirá todos los detalles disponibles, en particular la ***información*** necesaria para la identificación del sistema de IA no conforme, el origen del sistema de IA ***y la cadena de suministro, la*** naturaleza del supuesto incumplimiento y el riesgo que entraña, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos esgrimidos por el agente económico pertinente. En particular, las autoridades de vigilancia del mercado indicarán si el incumplimiento se debe a uno o varios de los siguientes factores:

(a) incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5;

(b) el incumplimiento por parte de ***un*** sistema de IA ***de alto riesgo*** de los requisitos establecidos en la sección 2 del capítulo III;

(c) las deficiencias de las normas armonizadas o especificaciones comunes contempladas en los artículos 40 y 41 que confieren una presunción de conformidad;

(d) incumplimiento del artículo 50.

7. Las autoridades de vigilancia del mercado de los Estados miembros distintas de la autoridad de vigilancia del mercado del Estado miembro que haya iniciado el procedimiento informarán sin demora indebida a la Comisión y a los demás Estados miembros de toda medida que adopten y de cualquier dato adicional sobre la no conformidad del sistema de IA de que dispongan y, en caso de desacuerdo con la medida nacional notificada, presentarán sus objeciones al respecto.

8. Cuando, en el plazo de tres meses a partir de la recepción de la ***notificación a que se refiere*** el apartado 5 del presente artículo, ni ***una autoridad de vigilancia del mercado de*** un Estado miembro ni la Comisión hayan formulado objeciones con respecto a una medida provisional adoptada por una ***autoridad de vigilancia del mercado de otro*** Estado miembro, dicha medida se considerará justificada. Ello se entenderá sin perjuicio de los derechos procesales del agente económico afectado de conformidad con el artículo 18 del Reglamento (UE) 2019/1020. ***El plazo de tres meses a que se refiere el presente apartado se reducirá a 30 días en caso de incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5 del presente Reglamento.***

9. Las autoridades de vigilancia del mercado de los Estados miembros velarán por que se adopten las medidas restrictivas adecuadas con respecto al producto ***o al sistema de IA*** en cuestión, como la retirada del producto ***o del sistema de IA*** de su mercado, sin demoras indebidas.

Artículo 80

Procedimiento para tratar los sistemas de IA clasificados por el proveedor como de riesgo no alto en aplicación del anexo III

1. *Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA clasificado por el proveedor como de no alto riesgo con arreglo al artículo 6, apartado 3, I es efectivamente de alto riesgo, la autoridad de vigilancia del mercado llevará a cabo una evaluación del sistema de IA en cuestión con respecto a su clasificación como sistema de IA de alto riesgo basándose en las condiciones establecidas en el artículo 6, apartado 3, y en las directrices de la Comisión.*

2. *Cuando, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA en cuestión es de alto riesgo, exigirá sin demora indebida al proveedor correspondiente que tome todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en un plazo que la autoridad de vigilancia del mercado podrá fijar.*

3. *Cuando la autoridad de vigilancia del mercado considere que el uso del sistema de IA en cuestión no se limita a su territorio nacional, informará sin demora indebida a la Comisión y a los demás Estados miembros de los resultados de la evaluación y de las medidas que ha exigido que adopte el proveedor.*

4. *El proveedor velará por que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento. Cuando el proveedor de un sistema de IA de que se trate no haga que el sistema de IA cumpla dichos requisitos y obligaciones en el plazo a que se refiere el apartado 2 del presente artículo, se le impondrán multas de conformidad con el artículo 99.*

5. *El proveedor velará por que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión.*

6. *Cuando el proveedor del sistema de IA de que se trate no adopte las medidas correctoras adecuadas en el plazo mencionado en el apartado 2 del presente artículo, se aplicarán los apartados 5 a 9 del artículo 79.*

7. *2. Cuando, en el transcurso de la evaluación realizada con arreglo al apartado 1 del presente artículo, la autoridad de vigilancia del mercado establezca que el sistema de IA ha sido clasificado erróneamente por el proveedor como de no alto riesgo con el fin de eludir la aplicación de los requisitos de la sección 2 del capítulo III, el proveedor estará sujeto al pago de multas de conformidad con el artículo 99.*

8. ***En el ejercicio de su facultad de supervisar la aplicación del presente artículo, y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar las comprobaciones oportunas, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 71 del presente Reglamento.***

Artículo 81

Procedimiento de salvaguardia de la Unión

1. Cuando, en un plazo de tres meses a partir de la recepción de la notificación a que se refiere el artículo 79, apartado 5, ***o de 30 días en caso de incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5, la autoridad de vigilancia del mercado de*** un Estado miembro plantee objeciones a una medida adoptada por otra ***autoridad de vigilancia del mercado,*** o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión consultará sin demora ***indebida*** a la ***autoridad de vigilancia del mercado del*** Estado miembro pertinente y al agente u operadores, y evaluará la medida nacional. Sobre la base de los resultados de dicha evaluación, la Comisión, en un plazo de ***seis*** meses, ***o de 60 días en caso de incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5, a partir*** de la notificación a que se refiere el artículo 79, apartado 5, decidirá si la medida nacional está justificada y notificará su decisión a la ***autoridad de vigilancia del mercado del*** Estado miembro de que se trate. ***La Comisión informará asimismo de su decisión a todas las demás autoridades de vigilancia del mercado.***

2. Cuando la Comisión considere que la ***medida adoptada por el Estado miembro pertinente está justificada***, todos los Estados miembros ***velarán por adoptar las*** medidas ***restrictivas adecuadas*** con ***respecto al sistema de*** IA ***en cuestión, como exigir la retirada del sistema de IA*** de su mercado ***sin demoras indebidas, e informarán*** de ello a la Comisión. Cuando la Comisión considere que la medida nacional no está justificada, el Estado miembro afectado retirará la medida ***e informará de ello a la Comisión***.

3. Cuando la medida nacional se considere justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) nº 1025/2012.

Artículo 82

Sistemas de IA que presentan un riesgo

1. Cuando, habiendo realizado una evaluación con arreglo al artículo 79, ***previa consulta a la autoridad pública nacional pertinente a que se refiere el artículo 77, apartado 1,*** la autoridad de vigilancia del mercado de un Estado miembro compruebe que, aunque un sistema de IA ***de alto riesgo*** es conforme con el presente Reglamento, presenta, no obstante, un riesgo para la salud o la seguridad de las personas, ▌ para los derechos fundamentales de las personas***,*** o para otros aspectos de la protección del interés público, exigirá al agente económico pertinente que adopte todas las medidas adecuadas para garantizar que el sistema de IA en cuestión, cuando se comercialice o se ponga en servicio, deje de presentar ese riesgo ***sin dilaciones indebidas,*** en un plazo ▌ que podrá fijar.

2. El proveedor u otro operador pertinente velará por que se adopten medidas correctoras en relación con todos los sistemas de IA afectados que haya puesto a disposición en el mercado de la Unión dentro del plazo prescrito por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. Los ***Estados miembros*** informarán inmediatamente a la Comisión y a los demás Estados miembros de las constataciones a que se refiere el apartado 1. Dicha información incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del sistema de IA de que se trate, el origen y la cadena de suministro del sistema de IA, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión consultará sin demora ***indebida*** al Estado o Estados miembros ***afectados*** y a los operadores pertinentes, y evaluará las medidas nacionales adoptadas. Sobre la base de los resultados de dicha evaluación, la Comisión decidirá si la medida está justificada y, en su caso, propondrá otras medidas adecuadas.

5. La Comisión ***comunicará inmediatamente*** su decisión a los Estados miembros. ***afectados y a los operadores pertinentes***. ***También informará a los demás Estados miembros.***

Artículo 83

Incumplimiento formal

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro llegue a una de las siguientes conclusiones, exigirá al proveedor en cuestión que ponga fin al incumplimiento de que se trate***, en un plazo que podrá fijar***:

   (a) se ha colocado un marcado ***CE*** infringiendo el artículo 48;

   (b) no se ha colocado el marcado ***CE***;

   (c) no se ha elaborado una declaración UE de conformidad;

   (d) no se ha redactado correctamente una declaración UE de conformidad;

   (e) no se ha llevado a cabo el registro en la base de datos de la UE;

   (f) en su caso, no se ha designado a un representante autorizado;

   (g) no se dispone de documentación técnica.

2. Si persiste el incumplimiento a que se refiere el apartado 1, la ***autoridad de vigilancia del mercado del*** Estado miembro en cuestión adoptará ***las*** medidas ***adecuadas y proporcionadas*** para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para garantizar su recuperación o retirada del mercado ***sin demora***.

Artículo 84

Estructuras de apoyo a las pruebas de IA de la Unión

1. *La Comisión designará una o varias estructuras de apoyo a las pruebas de IA de la Unión para realizar las tareas enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 2019/1020 en el ámbito de la IA.*

2. *2. Sin perjuicio de las tareas mencionadas en el apartado 1, las estructuras de apoyo a las pruebas de IA de la Unión también proporcionarán asesoramiento técnico o científico independiente a petición de la Junta Directiva, la Comisión o las autoridades de vigilancia del mercado.*

Sección

4

Recursos

Artículo 85

Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado

Sin perjuicio de otros recursos administrativos o judiciales, cualquier persona física o jurídica que tenga motivos para considerar que se han infringido las disposiciones del presente Reglamento podrá presentar reclamaciones motivadas ante la autoridad de vigilancia del mercado competente.

De conformidad con el Reglamento (UE) 2019/1020, dichas reclamaciones se tendrán en cuenta a efectos de la realización de actividades de vigilancia del mercado, y se tramitarán en consonancia con los procedimientos específicos establecidos al respecto por las autoridades de vigilancia del mercado.

Artículo 86

Derecho a una explicación de la toma de decisiones individual

1. *Toda persona afectada que sea objeto de una decisión adoptada por el responsable del despliegue sobre la base de los resultados de un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o afecte significativamente de manera similar a dicha persona de forma que considere que tiene un impacto negativo en su salud, seguridad o derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas sobre el papel del sistema de IA en el procedimiento de toma de decisiones y sobre los principales elementos de la decisión adoptada.*

2. *El apartado 1 no se aplicará al uso de sistemas de IA para los que se deriven excepciones o restricciones a la obligación establecida en el apartado 1 del Derecho de la Unión o nacional en cumplimiento del Derecho de la Unión.*

3. *El presente artículo sólo se aplicará en la medida en que el derecho contemplado en el apartado 1 no esté previsto de otro modo en el Derecho de la Unión.*

Artículo 87

Notificación de infracciones y protección de los denunciantes

La Directiva (UE) 2019/1937 se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien dichas infracciones.

Sección 5

Supervisión, investigación, ejecución y control de los proveedores de modelos de IA de uso general

Artículo 88

Cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general

1. ***La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el Capítulo V, teniendo en cuenta las garantías procesales del artículo 94. La Comisión confiará la ejecución de estas tareas a la Oficina AI, sin perjuicio de las facultades de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión basado en los Tratados.***

2. ***Sin perjuicio de lo dispuesto en el apartado 3 del artículo 75, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las competencias establecidas en la presente sección, cuando ello sea necesario y proporcionado para ayudarles en el cumplimiento de sus funciones con arreglo al presente Reglamento.***

Artículo 89

Acciones de control

1. *Para llevar a cabo las tareas que le asigna la presente sección, la Oficina de IA podrá adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida su adhesión a los códigos de prácticas aprobados.*

2. *Los proveedores intermedios tendrán derecho a presentar una denuncia por presunta infracción del presente Reglamento. La denuncia deberá estar debidamente motivada e indicar como mínimo:*

   (a) *el punto de contacto del proveedor del modelo de IA de propósito general de que se trate;*

   (b) *una descripción de los hechos pertinentes, las disposiciones del presente Reglamento de que se trate y la razón por la que el proveedor intermedio considera que el proveedor del modelo de IA de propósito general de que se trate ha infringido el presente Reglamento;*

   (c) *cualquier otra información que el proveedor intermedio que envió la solicitud considere pertinente, incluida, en su caso, la información recabada por iniciativa propia.*

Artículo 90

Alertas de riesgos sistémicos por el panel científico

1. La comisión técnica científica puede proporcionar una alerta cualificada a la Oficina de AI cuando tenga motivos para sospechar que:

(a) un modelo de IA de propósito general plantea un riesgo concreto identificable a nivel de la Unión; o,

(b) un modelo de IA de propósito general cumple los requisitos contemplados en el artículo 51 .

2. A partir de dicha descripción cualificada, la Comisión, a través de la Oficina AI y tras haber informado a la Junta, podrá ejercer las competencias establecidas en el presente Capítulo a efectos de evaluar el asunto. La Oficina de AI informará al Consejo de cualquier medida adoptada con arreglo a los artículos 91 a 94.

3. Una descripción cualificada deberá estar debidamente motivada e indicar como mínimo:

(a) el punto de contacto del proveedor del modelo de IA de propósito general con el riesgo sistémico en cuestión;

(b) una descripción de los hechos pertinentes y los motivos de la descripción por parte de la comisión técnica científica;

(c) cualquier otra información que la comisión técnica científica considere pertinente, incluida, en su caso, la información recabada por iniciativa propia.

Artículo 91

Facultad de solicitar documentación e información

1. La Comisión podrá solicitar al proveedor del modelo de IA de propósito general de que se trate que facilite la documentación elaborada por el proveedor con arreglo a los artículos 53 y 55, o cualquier información adicional que resulte necesaria a efectos de la evaluación del cumplimiento del presente Reglamento por parte del proveedor.

2. Antes de enviar la solicitud de información, la Oficina de IA podrá iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general.

3. Previa solicitud debidamente justificada de la comisión técnica científica, la Comisión podrá emitir una solicitud de información a un proveedor de un modelo de IA de propósito general, cuando el acceso a la información sea necesario y proporcionado para el cumplimiento de las tareas de la comisión técnica científica con arreglo al artículo 68, apartado 2.

4. En la solicitud de información se indicará la base jurídica y el objeto de la solicitud, se especificará qué información se requiere y se fijará un plazo para facilitarla, y se indicarán las multas previstas en el artículo 101 por facilitar información incorrecta, incompleta o engañosa.

5. El proveedor del modelo de IA polivalente de que se trate, o su representante, facilitará la información solicitada. En el caso de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas autorizadas a representarlas por ley o por sus estatutos facilitarán la información solicitada en nombre del proveedor del modelo de IA polivalente de que se trate. Los abogados debidamente autorizados para actuar podrán facilitar información en nombre de sus clientes. No obstante, los clientes seguirán siendo plenamente responsables si la información facilitada es incompleta, incorrecta o engañosa.

Artículo 92

Poder para realizar evaluaciones

1. La Oficina de IA, previa consulta al Consejo, podrá realizar evaluaciones del modelo de IA de propósito general de que se trate:

(a) evaluar el cumplimiento por parte del prestador de las obligaciones derivadas del presente Reglamento, cuando la información recabada con arreglo al artículo 91 sea insuficiente; o,

(b) investigar los riesgos sistémicos a nivel de la Unión de los modelos de IA de propósito general con riesgo sistémico, en particular a raíz de un informe cualificado de la comisión técnica científica de conformidad con el artículo 89, *apartado 1, letra a).*

2. La Comisión podrá decidir nombrar expertos independientes para que lleven a cabo evaluaciones en su nombre, incluso a partir del panel científico creado en virtud del artículo 68. Los expertos independientes designados para esta tarea deberán cumplir los criterios establecidos en el apartado 2 del artículo 68.

3. A efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de propósito general de que se trate a través de API u otros medios y herramientas técnicos adecuados, incluido el código fuente.

4. En la solicitud de acceso se indicará la base jurídica, el objeto y los motivos de la solicitud y se fijará el plazo en el que deberá facilitarse el acceso, así como las multas previstas en el artículo 101 en caso de que no se facilite el acceso.

5. Los proveedores del modelo de IA polivalente de que se trate y, en el caso de personas jurídicas, sociedades o empresas, o cuando carezcan de personalidad jurídica, las personas autorizadas a representarlas por ley o por sus estatutos, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA polivalente de que se trate.

6. La Comisión adoptará actos de ejecución en los que se establezcan las modalidades y condiciones de las evaluaciones, incluidas las modalidades de participación de expertos independientes, así como el procedimiento para su selección. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

7. Antes de solicitar acceso al modelo de IA de propósito general en cuestión, la Oficina de IA podrá iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general para recabar más información sobre las pruebas internas del modelo, las salvaguardias internas para prevenir riesgos sistémicos y otros procedimientos y medidas internas que el proveedor haya adoptado para mitigar dichos riesgos.

Artículo 93

Poder para solicitar medidas

1. Cuando sea necesario y oportuno, la Comisión podrá solicitar a los proveedores que:

(a) adoptar las medidas adecuadas para cumplir las obligaciones establecidas en el artículo 53;

(b) exigir a un proveedor que aplique medidas paliativas, cuando la evaluación realizada de conformidad con el artículo 92 haya suscitado una preocupación grave y justificada de riesgo sistémico a escala de la Unión;

(c) restringir la comercialización, retirar o recuperar el modelo.

2. Antes de solicitar una medida, la Oficina de IA puede iniciar un diálogo estructurado con el proveedor del modelo de IA de propósito general.

3. Si, durante el diálogo estructurado a que se refiere el apartado 2, el proveedor del modelo de IA de propósito general con riesgo sistémico ofrece compromisos de aplicar medidas de mitigación para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante decisión, hacer vinculantes dichos compromisos y declarar que no hay más motivos para actuar.

Artículo 94

Derechos procesales de los operadores económicos del modelo general de IA

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará *mutatis mutandis* a los proveedores del modelo de IA de propósito general, sin perjuicio de los derechos procesales más específicos previstos en el presente Reglamento.

CAPÍTULO X
CÓDIGOS DE CONDUCTA Y DIRECTRICES

Artículo 95

Códigos de conducta para la aplicación voluntaria de requisitos específicos

1. La ***Oficina de la IA*** y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta***, incluidos los mecanismos de gobernanza conexos,*** destinados a fomentar la aplicación voluntaria a los sistemas de IA, distintos de los sistemas de IA de alto riesgo, de ***algunos o todos los*** requisitos establecidos en el capítulo III, sección 2, teniendo en cuenta las ***soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos***.

2. La ***Oficina de la IA*** y los ***Estados*** miembros facilitarán ▌ la elaboración de códigos de conducta ***relativos a*** la aplicación voluntaria***, incluso por parte de los implantadores, de requisitos específicos a todos los*** sistemas de IA***, sobre la base de objetivos claros e indicadores clave de rendimiento para medir la consecución de dichos objetivos, incluidos elementos como, entre otros:***

(a) elementos aplicables previstos en las directrices éticas de la Unión para una IA fiable;

(b) evaluar y minimizar el impacto de los sistemas de IA en la sostenibilidad medioambiental, incluso en lo que se refiere a la programación eficiente desde el punto de vista energético y a las técnicas para el diseño, entrenamiento y uso eficientes de la IA;

(c) promover la alfabetización en IA, en particular la de las personas que se ocupan del desarrollo, el funcionamiento y el uso de la IA;

(d) facilitar un diseño inclusivo y diverso de los sistemas de IA, entre otras cosas mediante la creación de equipos de desarrollo inclusivos y diversos y el fomento de la participación de las partes interesadas en ese proceso;

(e) evaluar y prevenir el impacto negativo de los sistemas de IA sobre las personas o grupos de personas vulnerables, también en lo que respecta a la accesibilidad para las personas con discapacidad, así como sobre la igualdad de género.

3. Los códigos de conducta podrán ser elaborados por proveedores ***o implantadores*** individuales de sistemas de IA, por organizaciones que los representen o por ambos, incluso con la participación de los ***implantadores*** y de cualquier parte interesada y sus organizaciones representativas***, incluidas las organizaciones de la sociedad civil y el mundo académico***. Los códigos de conducta podrán abarcar uno o más sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes.

4. La ***Oficina de AI*** y los ***Estados miembros tendrán en cuenta*** los intereses y necesidades específicos de ***las PYME, incluidas*** las de nueva creación***,*** a la hora de fomentar y facilitar la elaboración de códigos de conducta.

Artículo 96

Directrices de la Comisión sobre la aplicación del presente Reglamento

1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:

(a) la aplicación de los requisitos y obligaciones contemplados en los artículos 8 a 15 y en el artículo 25;

(b) las prácticas prohibidas contempladas en el artículo 5;

(c) la aplicación práctica de las disposiciones relativas a la modificación sustancial;

(d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50;

(e) información detallada sobre la relación del presente Reglamento con la legislación de armonización de la Unión enumerada en el anexo I, así como con otra legislación pertinente de la Unión, incluso en lo que se refiere a la coherencia en su aplicación;

(f) la aplicación de la definición de sistema de IA que figura en el apartado 1 del artículo 3.

Al publicar dichas directrices, la Comisión prestará especial atención a las necesidades de las PYME, incluidas las de nueva creación, de las autoridades públicas locales y de los sectores que más puedan verse afectados por el presente Reglamento.

Las directrices a que se refiere el párrafo primero tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas establecidas en virtud de la legislación de armonización de la Unión.

2. A petición de los Estados miembros o de la Oficina de AI, o por iniciativa propia, la Comisión actualizará las directrices previamente adoptadas cuando lo considere necesario.

CAPÍTULO XI
DELEGACIÓN DE PODERES Y COMITOLOGÍA

Artículo 97

Ejercicio de la delegación

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. 1. Los ***poderes para adoptar actos delegados a que se refieren el*** artículo 6, apartado 6, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5***, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, se*** otorgan a la Comisión por un período de ***cinco años a partir de ...*** [***fecha de entrada*** en vigor del presente Reglamento]. La Comisión elaborará ***un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.***

3. La delegación de poderes a que se refieren el apartado 6 del artículo 6, los apartados 1 y 3 del artículo 7 y el apartado 3 del artículo 11,

Los apartados 5 y 6 del artículo 43, el apartado 5 del artículo 47***, el apartado 3 del artículo 51, el apartado 4 del artículo 52 y los apartados 5 y 6 del artículo 53*** podrán ser revocados en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de poderes que en ella se especifique. Surtirá efecto el día siguiente al de su publicación en el ***Diario Oficial de la Unión Europea*** o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de adoptar un acto delegado, la Comisión consultará a expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 "Legislar mejor".

5. Tan pronto como adopte un acto delegado, la Comisión lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Todo acto delegado adoptado en virtud del artículo 6, apartado 6, del artículo 7, apartados 1 y 3, del artículo 11, apartado 3, del artículo 43, apartados 5 y 6, el artículo 47, apartado 5***, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6,*** sólo entrarán en vigor si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. Este plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 98

Procedimiento de comité

1. 1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

CAPÍTULO XII
SANCIONES

Artículo 99

Sanciones

1. En cumplimiento de las condiciones establecidas en el presente Reglamento, los Estados miembros determinarán el régimen de sanciones ***y otras medidas coercitivas, que podrán incluir también advertencias y medidas no pecuniarias***, aplicables a las infracciones del presente Reglamento ***por parte de los operadores,*** y adoptarán todas las medidas necesarias para garantizar su aplicación correcta y eficaz***, teniendo en cuenta las directrices publicadas por la Comisión en virtud*** del artículo 96. Las sanciones previstas serán efectivas, proporcionadas y disuasorias. Tendrán en cuenta ▌ los intereses de las ***PYME, incluidas las de nueva creación,*** y su viabilidad económica.

2. Los Estados miembros notificarán sin demora a la Comisión, a ***más tardar en la fecha de entrada en vigor,*** el régimen de sanciones y las demás medidas de ejecución a que se refiere el apartado 1, así como cualquier modificación posterior de los mismos.

3. ***El incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5*** se sancionará con multas administrativas de hasta ***35 000 000*** EUR o, si el infractor es ***una empresa***, de hasta ***el 7*** % de su volumen de negocios total anual a escala mundial correspondiente al ejercicio anterior, si esta cifra es superior.

4. ▌El incumplimiento por parte de ***un*** sistema de IA de cualquiera ***de las siguientes disposiciones relativas a los operadores u organismos notificados***, distintas de las establecidas en los artículos 5 ▌, se sancionará con multas administrativas de hasta ***15 000 000*** EUR o, si el infractor es una empresa, de hasta ***15 000 000*** EUR.
el 3 % de su volumen de negocios total anual en todo el mundo durante el ejercicio anterior, si esta cifra es superior***:***

(a) obligaciones de los prestadores con arreglo al artículo 16;

(b) obligaciones de los representantes autorizados en virtud del artículo 22;

(c) obligaciones de los importadores con arreglo al artículo 23;

(d) obligaciones de los distribuidores con arreglo al artículo 24;

(e) obligaciones de los responsables del despliegue en virtud del artículo 26***;***

(f) requisitos y obligaciones de los organismos notificados con arreglo a los artículos 31, 33(1), 33(3), 33(4) o 34;

(g) obligaciones de transparencia para proveedores y usuarios con arreglo al artículo 50.

5. El suministro de información incorrecta, incompleta o engañosa a los organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud se castigará con multas administrativas de hasta ***7 500 000*** EUR o, si el infractor es una empresa, de hasta ***el 1*** % de su volumen de negocios total anual a escala mundial correspondiente al ejercicio anterior, si esta cifra es superior.

6. En el caso de las PYME, incluidas las de nueva creación, cada multa a que se refiere el presente artículo será de hasta los porcentajes o el importe a que se refieren los apartados 3, 4 y 5, si éste fuera inferior.

7. A la hora de decidir ***sobre la imposición de una*** multa administrativa ***y sobre*** su cuantía en cada caso concreto, se tendrán en cuenta todas las circunstancias pertinentes de la situación concreta y, en ***su caso, se tendrá*** en cuenta lo siguiente:

(a) la naturaleza, gravedad y duración de la infracción y de sus consecuencias***, teniendo en cuenta la finalidad del sistema de IA, así como, en su caso, el número de personas afectadas y el nivel de perjuicio sufrido por éstas***;

(b) si otras autoridades de vigilancia del mercado ***de uno o más Estados miembros*** ya han aplicado multas administrativas al mismo operador por la misma infracción***;***

(c) si otras autoridades ya han aplicado multas administrativas al mismo operador por infracciones de otro Derecho de la Unión o nacional, cuando tales infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;

(d) el tamaño***, el volumen de negocios anual*** y la cuota de mercado del operador que comete la infracción;

(e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, por la infracción;

(f) el grado de cooperación con las autoridades nacionales competentes, con el fin de remediar la infracción y mitigar los posibles efectos adversos de la misma;

(g) el grado de responsabilidad del operador teniendo en cuenta las medidas técnicas y organizativas aplicadas por él;

(h) la forma en que la infracción llegó a conocimiento de las autoridades nacionales competentes, en particular si el operador notificó la infracción y, en caso afirmativo, en qué medida;

(i) el carácter intencionado o negligente de la infracción;

(j) cualquier medida adoptada por el operador para mitigar el daño sufrido por las personas afectadas.

8. Cada Estado miembro establecerá normas sobre ▌ en qué medida podrán imponerse multas administrativas a las autoridades y organismos públicos establecidos en dicho Estado miembro.

9. En función del ordenamiento jurídico de los Estados miembros, las normas sobre multas administrativas podrán aplicarse de manera que las multas sean impuestas por los tribunales nacionales competentes ***o*** por otros organismos, según proceda en dichos Estados miembros. La aplicación de dichas normas en dichos Estados miembros tendrá un efecto equivalente.

10. El ejercicio por parte de la autoridad de vigilancia del mercado de sus competencias en virtud del presente artículo estará sujeto a las garantías procesales apropiadas de conformidad con el Derecho de la Unión y nacional, incluidos recursos judiciales efectivos y garantías procesales.

11. Los Estados miembros informarán anualmente a la Comisión sobre las multas administrativas que hayan impuesto durante ese año, de conformidad con el presente artículo, y sobre cualquier litigio o procedimiento judicial relacionado.

Artículo 100

Multas administrativas a las instituciones, órganos y organismos de la Unión

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, órganos y organismos de la Unión que entren en el ámbito de aplicación del presente Reglamento. Al decidir si se impone una multa administrativa y al decidir el importe de la multa administrativa en cada caso concreto, se tendrán en cuenta todas las circunstancias pertinentes de la situación específica y se prestará la debida atención a lo siguiente:

   (a) la naturaleza, gravedad y duración de la infracción y de sus consecuencias; teniendo en cuenta ***la finalidad del sistema de IA de que se trate, así como el número de personas afectadas y el nivel de perjuicio sufrido por ellas, y cualquier infracción anterior pertinente;***

(b) el grado de responsabilidad de la institución, órgano u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas por ellos;

(c) cualquier medida adoptada por la institución, órgano u organismo de la Unión para paliar los daños sufridos por las personas afectadas;

(d) el ***grado de*** cooperación con el Supervisor Europeo de Protección de Datos para remediar la infracción y mitigar los posibles efectos adversos de la misma, incluido el cumplimiento de cualquiera de las medidas previamente ordenadas por el Supervisor Europeo de Protección de Datos contra la institución, órgano u organismo de la Unión de que se trate en relación con el mismo asunto;

(e) cualquier infracción anterior similar cometida por la institución, órgano u organismo de la Unión;

(f) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución, órgano u organismo de la Unión notificó la infracción y, en caso afirmativo, en qué medida;

(g) el presupuesto anual de la institución, órgano u organismo de la Unión.

2. El ***incumplimiento de la prohibición de las prácticas de IA a que se refiere el artículo 5*** estará sujeto a multas administrativas de hasta ***1 500 000 EUR.***

▌

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones previstos en el presente Reglamento, distintos de los establecidos en los artículos 5 ▌, estará sujeto a multas administrativas de hasta ▌ ***750 000*** EUR.

4. Antes de adoptar decisiones en virtud del presente artículo, el Supervisor Europeo de Protección de Datos dará a la institución, órgano u organismo de la Unión que sea objeto del procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída sobre el asunto relativo a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en elementos y circunstancias sobre los que las partes afectadas hayan podido pronunciarse. Los denunciantes, si los hubiere, estarán estrechamente asociados al procedimiento.

5. En el procedimiento se respetarán plenamente los derechos de defensa de los interesados. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas o empresas en la protección de sus datos personales o secretos comerciales.

6. Los fondos recaudados mediante la imposición de multas en virtud del presente artículo ***contribuirán al presupuesto general*** de la Unión***. Las multas no afectarán al funcionamiento efectivo*** de la ***institución, órgano u organismo de la Unión sancionado***.

7. El Supervisor Europeo de Protección de Datos notificará anualmente a la Comisión las multas administrativas que haya impuesto en virtud del presente artículo y los litigios o procedimientos judiciales que haya incoado.

Artículo 101

Multas para los proveedores de modelos de IA de uso general

1. La Comisión podrá imponer a los proveedores de modelos de IA de propósito general multas que no superen el 3 % de su volumen de negocios total a nivel mundial en el ejercicio financiero anterior o 15 millones de euros, si esta cifra es superior, cuando la Comisión constate que el proveedor actuó de forma intencionada o negligente:

(a) infringido las disposiciones pertinentes del presente Reglamento;

(b) no haya atendido una solicitud de un documento o de información con arreglo al artículo 91, o haya facilitado información incorrecta, incompleta o engañosa;

(c) ha incumplido una medida solicitada en virtud del artículo 93;

(d) no haya puesto a disposición de la Comisión el acceso al modelo de IA de propósito general o al modelo de IA de propósito general con riesgo sistémico con vistas a realizar una evaluación con arreglo al artículo 92.

Para fijar el importe de la multa o de la multa coercitiva se tendrá en cuenta la naturaleza, gravedad y duración de la infracción, así como los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el apartado 3 del artículo 93 o contraídos en los códigos de prácticas pertinentes de conformidad con el artículo 56.

2. Antes de adoptar la decisión con arreglo al apartado 1, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de propósito general o del modelo de IA de propósito general con riesgo sistémico y le dará la oportunidad de ser oído.

3. Las multas impuestas de conformidad con el presente artículo serán efectivas, proporcionadas y disuasorias.

4. La información sobre las multas impuestas en virtud del presente artículo también se comunicará al Consejo, según proceda.

5. El Tribunal de Justicia de la Unión Europea tendrá competencia jurisdiccional plena para revisar las decisiones de la Comisión por las que se fije una multa en virtud del presente artículo. Podrá anular, reducir o aumentar la multa impuesta.

6. La Comisión adoptará actos de ejecución que contengan disposiciones detalladas sobre los procedimientos con vistas a la posible adopción de decisiones de conformidad con el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO XIII
DISPOSICIONES FINALES

Artículo 102

Modificación del Reglamento (CE) nº 300/2008

En el artículo 4, apartado 3, del Reglamento (CE) nº 300/2008, se añade el párrafo siguiente

Al adoptar medidas detalladas relacionadas con las especificaciones técnicas y los procedimientos de homologación y utilización de equipos de seguridad relativos a sistemas de inteligencia artificial en el sentido del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 103

Modificación del Reglamento (UE) nº 167/2013

En el artículo 17, apartado 5, del Reglamento (UE) nº 167/2013, se añade el párrafo siguiente:

Al adoptar actos delegados con arreglo al párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

\+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 104

Modificación del Reglamento (UE) nº 168/2013

En el artículo 22, apartado 5, del Reglamento (UE) nº 168/2013, se añade el párrafo siguiente:

Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 105

Modificación de la Directiva 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

5. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, al llevar a cabo sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3, la Comisión tendrá en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 106

Modificación de la Directiva (UE) 2016/797

En el artículo 5 de la Directiva (UE) 2016/797, se añade el párrafo siguiente:

12. Al adoptar actos delegados con arreglo al apartado 1 y actos de ejecución con arreglo al apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

\+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 107

Modificación del Reglamento (UE) 2018/858

En el artículo 5 del Reglamento (UE) 2018/858 se añade el siguiente apartado:

4. Al adoptar actos delegados con arreglo al apartado 3 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 108

Modificación del Reglamento (UE) 2018/1139

El Reglamento (UE) 2018/1139 queda modificado como sigue:

(1) en el artículo 17, se añade el párrafo siguiente

3. Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución con arreglo al apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/... del Parlamento Europeo y del Consejo*+, se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)";

(2) en el artículo 19, se añade el párrafo siguiente

4. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/...++**, se tendrán en cuenta los** requisitos establecidos en el título III, capítulo 2, de dicho Reglamento";

\+ DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

++ DO: Insértese el número del presente Reglamento (2021/0106(COD)).

(3) en el artículo 43, se añade el párrafo siguiente

4. Al adoptar actos de ejecución con arreglo al apartado 1 en relación con sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/...[+], **se tendrán en cuenta** los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento";

(4) en el artículo 47, se añade el párrafo siguiente

3. Cuando se adopten actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/...[+], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento";

(5) en el artículo 57, se añade el párrafo siguiente

Al adoptar los actos de ejecución relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/...[+], **se tendrán en cuenta los** requisitos establecidos en el capítulo 2 del título III de dicho Reglamento";

[+] DO: Insértese el número del presente Reglamento (2021/0106(COD)).

(6) en el artículo 58, se añade el párrafo siguiente

3. Cuando se adopten actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) nº 2024/...[+], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento".

Artículo 109

Modificación del Reglamento (UE) 2019/2144

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el párrafo siguiente:

3. Al adoptar los actos de ejecución con arreglo al apartado 2, relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo*[++], se tendrán en cuenta los requisitos establecidos en el capítulo 2 del título III de dicho Reglamento.

---

* Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo, de ..., por el que se establecen normas armonizadas sobre la inteligencia artificial (acto relativo a la inteligencia artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)".

[+] DO: Insértese el número del presente Reglamento (2021/0106(COD)).

[++] DO: Insértese en el texto el número del presente Reglamento (2021/0106(COD)) y complétese la correspondiente nota a pie de página.

Artículo 110

Modificación de la Directiva (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del **Consejo61** ***, se añade el punto siguiente:***

'***(68)*** Reglamento ***(UE) 2024/... del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (DO L, ..., ELI: ...)***".

61 Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

Artículo 111

Sistemas de IA ya comercializados o puestos en servicio

1. ***Sin perjuicio de la aplicación del artículo 5 a que se refiere el artículo*** 113, apartado 3, letra a)***,*** los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en el anexo X que hayan sido comercializados o puestos en servicio antes del

▌... [36 meses a partir de la fecha de entrada en vigor del presente Reglamento***/ se pondrán en conformidad con el presente Reglamento a más tardar el 31 de diciembre de 2030***.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta ▌ en la evaluación de cada sistema informático de gran magnitud establecido por los actos jurídicos enumerados en el anexo X que deba llevarse a cabo conforme a lo dispuesto en dichos actos jurídicos ***y cuando estos sean sustituidos o modificados***.

2. ***Sin perjuicio de la aplicación del artículo 5 a que se refiere el artículo*** 113, apartado 3, letra a)***,*** el presente Reglamento se aplicará a los ***operadores de*** sistemas de IA de alto riesgo, distintos de los sistemas a que se refiere el apartado 1 del presente artículo, que hayan sido comercializados o puestos en servicio antes del ... [24 meses a partir de la fecha de entrada en vigor del presente Reglamento], únicamente si, a partir de esa fecha, dichos sistemas son objeto de cambios significativos en sus ***diseños. En el caso de los sistemas de IA de alto riesgo*** destinados a ser ***utilizados por las autoridades públicas, los proveedores e implantadores de dichos sistemas adoptarán las medidas necesarias para cumplir los requisitos del presente Reglamento antes de ...***[***seis años a partir de la fecha de entrada en vigor del presente Reglamento***]***.***

3. ***Los proveedores de modelos de IA de uso general que se hayan comercializado antes del ... [12*** meses a partir de la fecha de entrada en vigor del presente Reglamento] ***adoptarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el ... [36 meses*** a partir de la fecha de entrada en vigor del presente Reglamento***]***.

Artículo 112

Evaluación y revisión

1. La Comisión evaluará la necesidad de modificar la lista del anexo III ***y la lista de prácticas de IA prohibidas del artículo 5,*** una vez al año tras la entrada en vigor del presente Reglamento ***y hasta el final del período de delegación de poderes establecido en el artículo 97***. La Comisión presentará los resultados de dicha evaluación al Parlamento Europeo y al Consejo. ***La Comisión presentará los resultados de dicha evaluación al Parlamento Europeo y al Consejo.***

2. A más tardar ... ***[cuatro años a partir de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, cada cuatro años, la Comisión evaluará e informará al Parlamento Europeo y al Consejo sobre lo siguiente:***

(a) la necesidad de modificar la ampliación de los epígrafes existentes o de añadir nuevos epígrafes en el anexo III;

(b) modificaciones de la lista de sistemas de IA que requieren medidas adicionales de transparencia en el artículo 50;

(c) enmiendas que mejoren la eficacia del sistema de supervisión y gobernanza.

3. A más tardar el ... ***[***cuatro años después de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento***. El informe incluirá una evaluación de la estructura de aplicación y de la posible necesidad de una agencia de la Unión para resolver las deficiencias detectadas. Sobre la base de los resultados, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento***. Los informes se harán públicos.

4. Los informes mencionados en el apartado 2 dedicarán una atención específica a los siguientes aspectos:

(a) la situación de los recursos financieros***, técnicos*** y humanos de las autoridades nacionales competentes para desempeñar eficazmente las tareas que les asigna el presente Reglamento;

(b) el estado de las sanciones, en particular las multas administrativas contempladas en el apartado 1 del artículo 99, aplicadas por los Estados miembros por las infracciones del presente Reglamento;

(c) adoptado normas armonizadas y especificaciones comunes desarrolladas en apoyo del presente Reglamento;

(d) el número de empresas que se incorporan al mercado tras la entrada en aplicación del presente Reglamento, y cuántas de ellas son PYME.

5. A más tardar el ... [cuatro años a partir de la fecha de entrada en vigor del presente Reglamento)], la Comisión evaluará el funcionamiento de la Oficina de Inteligencia Artificial, si se le han otorgado poderes y competencias suficientes para cumplir sus tareas y si sería pertinente y necesario para la correcta aplicación y cumplimiento del presente Reglamento mejorar la Oficina de Inteligencia Artificial y sus competencias de ejecución y aumentar sus recursos. La Comisión presentará este informe de evaluación al Parlamento Europeo y al Consejo.

6. A más tardar el ... [cuatro años a partir de la fecha de entrada en vigor del presente Reglamento)] y, a continuación, cada cuatro años, la Comisión presentará un informe sobre la revisión de los progresos realizados en la elaboración de productos de normalización sobre el desarrollo energéticamente eficiente de modelos de uso general, y evaluará la necesidad de nuevas medidas o acciones, incluidas medidas o acciones vinculantes. El informe se presentará al Parlamento Europeo y al Consejo y se hará público.

7. A más tardar **...** [***cuatro años*** a partir de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, cada ***tres*** años, la Comisión evaluará el impacto y la eficacia de los códigos de conducta ***voluntarios*** para fomentar la aplicación de los requisitos establecidos en el capítulo II, sección 2, ***para los sistemas de*** IA distintos de los sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para los sistemas de IA distintos de los sistemas de IA de alto riesgo***, también en lo que respecta a la sostenibilidad medioambiental.***

8. A efectos de los apartados 1 a 7, la Junta, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión a petición de ésta ***y sin demora injustificada.***

9. Al llevar a cabo las evaluaciones y revisiones a que se refieren los apartados 1 a 7, la Comisión tendrá en cuenta las posiciones y conclusiones de la Junta, del Parlamento Europeo, del Consejo y de otros organismos o fuentes pertinentes.

10. En caso necesario, la Comisión presentará propuestas adecuadas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología***, el efecto de los sistemas de IA en la salud y la seguridad, y en los derechos fundamentales,*** y a la luz del estado de avance de la sociedad de la información.

11. Para orientar las evaluaciones y revisiones a que se refieren los apartados 1 a 7 del presente artículo, la Oficina de AI se comprometerá a desarrollar una metodología objetiva y participativa para la evaluación de los niveles de riesgo basada en los criterios expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en:

(a) la lista del anexo III, incluida la ampliación de los epígrafes de zona existentes o la adición de nuevos epígrafes de zona en dicho anexo;

(b) la lista de prácticas prohibidas establecida en el artículo 5; y,

(c) la lista de sistemas de IA que requieren medidas adicionales de transparencia de conformidad con el artículo 50.

12. Cualquier modificación del presente Reglamento con arreglo al apartado 10, o de los actos delegados o de ejecución pertinentes, que se refiera a la legislación sectorial de armonización de la Unión enumerada en la sección B del anexo I tendrá en cuenta las especificidades reglamentarias de cada sector, así como los mecanismos y autoridades existentes en materia de gobernanza, evaluación de la conformidad y ejecución establecidos en el mismo.

13. A más tardar el ... [siete años a partir de la fecha de entrada en vigor del presente Reglamento], la Comisión llevará a cabo una evaluación de la aplicación del presente Reglamento e informará al respecto al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del presente Reglamento. Sobre la base de los resultados, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que se refiere a la estructura de aplicación y a la necesidad de una agencia de la Unión para resolver las deficiencias detectadas.

Artículo 113

Entrada en vigor y aplicación

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Se aplicará a partir de ... [24 meses después de la fecha de entrada en vigor del presente Reglamento]. No obstante:

▌

(a) Los capítulos I y II se aplicarán a partir de ... [seis meses después de la fecha de entrada en vigor del presente Reglamento];

(b) El capítulo III ▌ sección 4***,*** el capítulo V, el capítulo VII ***y el capítulo XII*** se aplicarán a partir del

... [***12*** meses a partir de la fecha de entrada en vigor del presente Reglamento], ***a excepción del artículo 101***;

(c) ***El apartado 1*** del artículo ***6 y las obligaciones correspondientes del presente Reglamento*** se aplicarán a partir del

... [***36*** meses a partir de la fecha de entrada en vigor del presente Reglamento].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. Hecho en ...,

Por el Parlamento El *EuropeoPor el Consejo PresidenteEl Presidente*

ANEXO I

Lista de la legislación de armonización de la Unión

Sección A. Lista de la legislación de armonización de la Unión basada en el nuevo marco legislativo

1. Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24) [derogada por el Reglamento sobre máquinas];

2. Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes (DO L 170 de 30.6.2009, p. 1);

3. Directiva 2013/53/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, relativa a embarcaciones de recreo y motos acuáticas y por la que se deroga la Directiva 94/25/CE (DO L 354 de 28.12.2013, p. 90);

4. Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros relativas a los ascensores y componentes de seguridad para ascensores (DO L 96 de 29.3.2014, p. 251);

5. Directiva 2014/34/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas (DO L 96 de 29.3.2014, p. 309);

6. Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre la armonización de las legislaciones de los Estados miembros relativas a la comercialización de equipos radioeléctricos y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014,
p. 62);

7. Directiva 2014/68/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos a presión (DO L 189 de 27.6.2014, p. 164);

8. Reglamento (UE) 2016/424 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las instalaciones de transporte por cable y por el que se deroga la Directiva 2000/9/CE (DO L 81 de 31.3.2016, p. 1);

9. Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo (DO L 81 de 31.3.2016, p. 51);

10. Reglamento (UE) 2016/426 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre los aparatos de gas y por el que se deroga la Directiva 2009/142/CE (DO L 81 de 31.3.2016, p. 99);

11. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1);

12. Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios para diagnóstico *in vitro* y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

Sección B. Lista de otra legislación de armonización de la Unión

13. Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo de 11 de marzo de 2008 sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) nº 2320/2002 (DO L 97 de 9.4.2008, p. 72);

14. Reglamento (UE) nº 168/2013 del Parlamento Europeo y del Consejo de 15 de enero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos de dos o tres ruedas y los cuatriciclos (DO L 60 de 2.3.2013, p. 52);

15. Reglamento (UE) nº 167/2013 del Parlamento Europeo y del Consejo de 5 de febrero de 2013, sobre la homologación y la vigilancia del mercado de los vehículos agrícolas y forestales (DO L 60 de 2.3.2013, p. 1);

16. Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos y por la que se deroga la Directiva 96/98/CE del Consejo (DO L 257 de 28.8.2014, p. 146);

17. Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea (DO L 138 de 26.5.2016, p. 44);

18. Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1);

19. Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de de 27 de noviembre de 2019, sobre los requisitos de homologación de tipo de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, en lo relativo a su seguridad general y a la protección de los ocupantes de vehículos y usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 78/2009, (CE) nº 79/2009 y (CE) nº 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010 de la Comisión, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012 y (UE) 2015/166 (DO L 325 de 16.12.2019, p. 1);

20. Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea y se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010, (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1), por lo que respecta al diseño, la producción y la comercialización de las aeronaves a que se refiere su artículo 2, apartado 1, letras a) y b), cuando se trate de aeronaves no tripuladas y de sus motores, hélices, piezas y equipos para controlarlas a distancia.

ANEXO II

Lista de infracciones penales contempladas en el artículo 5, apartado 1, letra e), inciso iii):

– ***terrorismo,***

– ***trata de seres humanos,***

– ***explotación sexual de menores y pornografía infantil,***

– ***tráfico ilícito de estupefacientes o sustancias psicotrópicas,***

– ***tráfico ilícito de armas, municiones o explosivos,***

– ***asesinato, lesiones corporales graves,***

– ***comercio ilícito de órganos o tejidos humanos,***

– ***tráfico ilícito de materiales nucleares o radiactivos,***

– ***secuestro, retención ilegal o toma de rehenes,***

– ***crímenes de la competencia de la Corte Penal Internacional,***

– ***apoderamiento ilícito de aeronaves o buques,***

– ***violación,***

– ***delitos contra el medio ambiente,***

– ***robo organizado o a mano armada,***

– ***sabotaje,***

– ***participación en una organización delictiva implicada en uno o varios de los delitos enumerados anteriormente.***

ANEXO III

Sistemas de IA de alto riesgo contemplados en el artículo 6, apartado 2

Los sistemas de IA de alto riesgo con arreglo al apartado 2 del artículo 6 son los sistemas de IA enumerados en cualquiera de los siguientes ámbitos:

1. ***Datos biométricos, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente:***

   (a) ***sistemas de identificación biométrica a distancia.***

   Esto no incluirá los sistemas de IA destinados a ser utilizados para la ***verificación biométrica cuyo único propósito sea confirmar que una persona*** física específica ***es la persona que dice ser***;

   (b) Sistemas de IA destinados a ser utilizados para la categorización biométrica, según atributos o características sensibles o protegidos basados en la inferencia de dichos atributos o características;

   (c) Sistemas de IA destinados al reconocimiento de emociones.

2. ▌Infraestructuras críticas:

(a) Sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y explotación de ***infraestructuras digitales críticas, el*** tráfico rodado o el suministro de agua, gas, calefacción o electricidad.

3. Educación y formación profesional:

(a) Sistemas de IA destinados a ser utilizados ***para determinar el acceso o la admisión o para asignar***

personas físicas a instituciones educativas y de formación profesional ***de todos los niveles***;

(b) Sistemas de IA destinados a ser utilizados ***para evaluar los resultados del aprendizaje, incluso cuando dichos resultados se utilizan para dirigir el proceso de aprendizaje de personas físicas en centros educativos y de formación profesional de todos los niveles***;

(c) Sistemas de IA destinados a ser utilizados con el fin de evaluar el nivel adecuado de educación que un individuo recibirá o al que podrá acceder, en el contexto de o dentro de instituciones educativas y de formación profesional;

(d) Sistemas de IA destinados a ser utilizados para supervisar y detectar comportamientos prohibidos de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de ellos.

4. Empleo, gestión de trabajadores y acceso al autoempleo:

   (a) Sistemas de IA destinados a ser utilizados para la contratación o selección de personas físicas, en particular ***para publicar anuncios de empleo específicos, analizar y filtrar solicitudes de empleo y evaluar candidatos***;

   (b) Sistemas de IA destinados a ser utilizados ***para tomar*** decisiones ***que afecten a las condiciones de las relaciones laborales,*** la promoción o la finalización de relaciones contractuales laborales, ***para asignar tareas basadas en el comportamiento individual o en rasgos o características personales o para supervisar y evaluar el*** rendimiento y el comportamiento de las personas en dichas relaciones.

5. Acceso y disfrute de los servicios privados esenciales y de los servicios y prestaciones públicos ***esenciales***:

   (a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar el derecho de las personas físicas a prestaciones y ***servicios esenciales*** de asistencia pública***, incluidos*** los servicios ***sanitarios***, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios;

   (b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su puntuación crediticia***,*** con la excepción de los sistemas de IA ***utilizados con el fin de detectar fraudes financieros***;

(c) ***Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la tarificación en relación con las personas físicas en el caso de los seguros de vida y salud;***

(d) Sistemas de IA destinados a ***evaluar y clasificar llamadas de emergencia de personas físicas o a*** ser utilizados para despachar, o establecer la prioridad en el despacho de, servicios de primera respuesta de emergencia, incluidos los de ***policía,*** bomberos y ayuda médica***, así como de sistemas de triaje de pacientes de atención sanitaria de emergencia;***

6. Fuerzas y cuerpos de seguridad***, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente:***

(a) Sistemas de IA destinados a ser utilizados por las autoridades policiales o judiciales***, o en su nombre, o por instituciones, órganos u organismos de la Unión en apoyo de las autoridades policiales o judiciales o en su nombre,*** para evaluar el riesgo de que una persona física sea ***víctima*** de infracciones penales;

(b) Sistemas de IA destinados a ser utilizados por ***o en nombre de las*** autoridades policiales ***o por las instituciones, órganos u organismos de la Unión en apoyo de las autoridades policiales como polígrafos o herramientas similares;***

▌

(c) Sistemas de IA destinados a ser utilizados por las autoridades policiales o judiciales***, o en su nombre, o por las instituciones, órganos u organismos de la Unión, en apoyo de las autoridades policiales o judiciales para evaluar*** la fiabilidad de las pruebas en el curso de la investigación o el enjuiciamiento de infracciones penales;

(d) Sistemas de IA destinados a ser utilizados por las fuerzas y cuerpos de seguridad ***o en su nombre o por las instituciones, órganos u organismos de la Unión en apoyo de las fuerzas y cuerpos de seguridad para evaluar la probabilidad de que una persona física delinca o vuelva a delinquir no*** basados ***únicamente*** en la elaboración de perfiles de personas físicas a que se refiere el artículo 3, apartado 4, de la Directiva (UE) 2016/680, o ***para evaluar*** rasgos y características de la personalidad o comportamientos delictivos anteriores de personas físicas o grupos;

(e) Sistemas de IA destinados a ser utilizados por ***o en nombre de las autoridades policiales o por las instituciones, órganos u organismos de la Unión en apoyo de las*** autoridades policiales para la elaboración de perfiles de personas físicas a que se refiere el artículo 3, apartado 4, de la Directiva (UE) 2016/680 en el curso de la detección, investigación o enjuiciamiento de infracciones penales***.***

7. Gestión de la migración, el asilo y el control de fronteras***, en la medida en que su uso esté permitido por la legislación nacional o de la Unión pertinente***:

(a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes como polígrafos y herramientas similares***;***

(b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes ***o por las instituciones, órganos u organismos de la Unión, o en su nombre,*** para evaluar un riesgo, incluido un riesgo para la seguridad, un riesgo de ***migración*** irregular o un riesgo sanitario, planteado por una persona física que pretenda entrar o que haya entrado en el territorio de un Estado miembro;

c) los sistemas de IA destinados a ***ser utilizados por las autoridades públicas competentes o por las instituciones, órganos u organismos de la Unión, o en su nombre, para*** asistir a las autoridades públicas competentes en el examen de las solicitudes de asilo, visado o permiso de residencia y en las reclamaciones conexas relativas a la admisibilidad de las personas físicas que solicitan un estatuto***, incluidas las evaluaciones conexas de la fiabilidad de las pruebas;***

(d) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o en su nombre, incluidas las instituciones, órganos u organismos de la Unión, en el contexto de la gestión de la migración, el asilo o el control de fronteras, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje.

8. Administración de justicia y procesos democráticos:

(a) Sistemas de IA destinados a ***ser utilizados por una autoridad judicial o en su nombre para*** asistir a una autoridad judicial en la investigación e interpretación de hechos y de la ley y en la aplicación de la ley a un conjunto concreto de hechos, ***o a ser utilizados de forma similar en la resolución alternativa de litigios;***

(b) ***Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento de voto de personas físicas en el ejercicio de su voto en elecciones o referendos. Esto no incluye los sistemas de IA a cuyos resultados no están expuestas directamente las personas físicas, como las herramientas utilizadas para organizar, optimizar o estructurar campañas políticas desde un punto de vista administrativo o logístico.***

ANEXO IV

Documentación técnica contemplada en el apartado 1 del artículo 11

La documentación técnica a que se refiere el apartado 1 del artículo 11 contendrá como mínimo la siguiente información, según proceda para el sistema de IA pertinente:

1. Una descripción general del sistema de IA que incluya:

   (a) su finalidad, el ***nombre del proveedor*** y la versión del sistema ***que refleja su relación con las versiones anteriores;***

   (b) el modo en que el sistema de IA interactúa o puede utilizarse para interactuar con hardware o software***, incluidos otros sistemas de IA, que*** no formen parte del propio sistema de IA, cuando proceda;

   (c) las versiones de software o firmware pertinentes, y cualquier requisito relacionado con la actualización de versiones;

   (d) la descripción de todas las formas en que el sistema de IA se comercializa o se pone en servicio, ***como paquetes de software integrados en hardware, descargas o API***;

(e) la descripción del hardware en el que está previsto que se ejecute el sistema de IA;

(f) cuando el sistema de IA sea un componente de productos, fotografías o ilustraciones que muestren las características externas, el marcado y la disposición interna de dichos productos;

(g) una descripción básica de la interfaz de usuario proporcionada al desplegador;

(h) instrucciones de uso para el implantador***, y una descripción básica de la interfaz de usuario proporcionada al implantador,*** cuando proceda ▌ ;

2. Una descripción detallada de los elementos del sistema de IA y del proceso para su desarrollo, incluyendo:

(a) los métodos y pasos seguidos para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas preentrenados proporcionados por terceros y la forma en que fueron utilizados, integrados o modificados por el proveedor;

(b) las especificaciones de diseño del sistema, es decir, la lógica general del sistema de inteligencia artificial y de los algoritmos; las principales opciones de diseño, incluidos los fundamentos y las suposiciones realizadas, incluso con respecto a las personas o grupos de personas con respecto a los cuales se pretende utilizar el sistema; las principales opciones de clasificación; para qué se ha diseñado el sistema con el fin de optimizarlo y la importancia de los diferentes parámetros; la ***descripción de los resultados esperados y la calidad de los resultados del sistema; las*** decisiones sobre cualquier posible compensación realizada con respecto a las soluciones técnicas adoptadas para cumplir los requisitos establecidos en la sección 2 del capítulo III;

(c) la descripción de la arquitectura del sistema, explicando cómo los componentes de software se basan o se alimentan entre sí y se integran en el procesamiento global; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA;

(d) cuando proceda, los requisitos de datos en términos de fichas técnicas que describan las metodologías y técnicas de formación y los conjuntos de datos de formación utilizados, incluida ***una descripción general de estos*** conjuntos de datos, ***información sobre*** su ***procedencia,*** alcance y características principales; cómo se obtuvieron y seleccionaron los datos; procedimientos de etiquetado (por ejemplo, para el aprendizaje supervisado), metodologías de limpieza de datos (por ejemplo, detección de valores atípicos);

(e) evaluación de las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de los resultados de los sistemas de IA por parte de ***quienes los despliegan***, de conformidad con el artículo 13, apartado 3, letra d);

(f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su rendimiento, junto con toda la información pertinente relacionada con las soluciones técnicas adoptadas para garantizar la conformidad continua del sistema de IA con los requisitos pertinentes establecidos en la sección 2 del capítulo III;

(g) los procedimientos de validación y ensayo utilizados, incluida información sobre los datos de validación y ensayo utilizados y sus principales características; los parámetros utilizados para medir la precisión, la robustez ▌ y el cumplimiento de otros requisitos pertinentes establecidos en el capítulo III, sección 2, así como los impactos potencialmente discriminatorios; los registros de ensayo y todos los informes de ensayo fechados y firmados por las personas responsables, también en lo que respecta a los cambios predeterminados a que se refiere la letra f);

(h) medidas de ciberseguridad implantadas;

3. Información detallada sobre la supervisión, el funcionamiento y el control del sistema de IA, en particular con respecto a: sus capacidades y limitaciones de funcionamiento, incluidos los grados de precisión para las personas o grupos de personas específicos sobre los que está previsto utilizar el sistema y el nivel general de precisión esperado en relación con su finalidad prevista; los resultados imprevistos previsibles y las fuentes de riesgos para la salud y la seguridad, los derechos fundamentales y la discriminación en vista de la finalidad prevista del sistema de IA; las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de los sistemas de IA por parte de ***quienes los despliegan***; las especificaciones sobre los datos de entrada, según proceda;

4. Una descripción de la idoneidad de las métricas de rendimiento para el sistema de IA específico;

5. Una descripción detallada del sistema de gestión de riesgos de conformidad con el artículo 9;

6. Una descripción de los ***cambios relevantes realizados por el proveedor*** en el sistema a lo largo de su ciclo de vida;

7. Una lista de las normas armonizadas aplicadas total o parcialmente cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*; cuando no se hayan aplicado tales normas armonizadas, una descripción detallada de las soluciones adoptadas para cumplir los requisitos establecidos en la sección 2 del capítulo III, incluida una lista de otras normas y especificaciones técnicas pertinentes aplicadas;

8. Una copia de la declaración de conformidad de la UE;

9. Una descripción detallada del sistema establecido para evaluar el rendimiento del sistema de IA en la fase posterior a la comercialización de conformidad con el artículo 72, incluido el plan de seguimiento posterior a la comercialización mencionado en el apartado 3 del artículo 72.

ANEXO V

Declaración de conformidad de la UE

La declaración UE de conformidad a que se refiere el artículo 47 contendrá toda la información siguiente:

1. Nombre y tipo del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;

2. Nombre y dirección del proveedor o, en su caso, de su representante autorizado;

3. Una declaración de que la declaración UE de conformidad se expide bajo la exclusiva responsabilidad del proveedor;

4. Una declaración de que el sistema de IA es conforme con el presente Reglamento y, si procede, con cualquier otra norma pertinente de la Unión que prevea la expedición de una declaración UE de conformidad;

5. Cuando un sistema de IA implique el tratamiento de datos personales, una declaración de que dicho sistema de IA cumple los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680;

6. Referencias a cualquier norma armonizada pertinente utilizada o a cualquier otra especificación común en relación con la cual se declare la conformidad;

7. En su caso, nombre y número de identificación del organismo notificado, descripción del procedimiento de evaluación de la conformidad realizado e identificación del certificado expedido;

8. El lugar y la fecha de emisión de la declaración, el nombre y la función de la persona que la firmó, así como una indicación de para quién o en nombre de quién firmó esa persona, una firma.

ANEXO VI

Procedimiento de evaluación de la conformidad basado en el control interno

1. El procedimiento de evaluación de la conformidad basado en el control interno es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 4.

2. El proveedor verifica que el sistema de gestión de la calidad establecido cumple los requisitos del artículo 17.

3. El proveedor examina la información contenida en la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en la sección 2 del capítulo III.

4. El proveedor también verifica que el proceso de diseño y desarrollo del sistema de IA y su seguimiento postcomercialización, tal como se menciona en el artículo 72, son coherentes con la documentación técnica.

ANEXO VII

Conformidad basada en una evaluación del sistema de gestión de la calidad y en una evaluación de la documentación técnica

1. Introducción

La conformidad basada en una evaluación del sistema de gestión de la calidad y una evaluación de la documentación técnica es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 5.

2. Visión general

El sistema de gestión de la calidad aprobado para el diseño, desarrollo y ensayo de sistemas de IA con arreglo al artículo 17 se examinará de conformidad con el punto 3 y se someterá a la vigilancia especificada en el punto 5. La documentación técnica del sistema de IA se examinará de conformidad con el punto 4.

3. Sistema de gestión de la calidad

3.1. La solicitud del proveedor deberá incluir:

(a) el nombre y la dirección del prestador y, si la solicitud la presenta un representante autorizado, también su nombre y dirección;

(b) la lista de sistemas de IA cubiertos por el mismo sistema de gestión de la calidad;

(c) la documentación técnica de cada sistema de IA incluido en el mismo sistema de gestión de la calidad;

(d) la documentación relativa al sistema de gestión de la calidad, que abarcará todos los aspectos enumerados en el artículo 17;

(e) una descripción de los procedimientos establecidos para garantizar que el sistema de gestión de la calidad sigue siendo adecuado y eficaz;

(f) una declaración escrita de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de gestión de la calidad será evaluado por el organismo notificado, que determinará si cumple los requisitos contemplados en el artículo 17.

La decisión se notificará al prestador o a su representante autorizado.

La notificación incluirá las conclusiones de la evaluación del sistema de gestión de la calidad y la decisión de evaluación motivada.

3.3. El sistema de gestión de la calidad aprobado deberá seguir siendo aplicado y mantenido por el proveedor para que siga siendo adecuado y eficaz.

3.4. El proveedor comunicará al organismo notificado cualquier modificación prevista del sistema de gestión de la calidad aprobado o de la lista de sistemas de gestión de la calidad cubiertos por éste.

Las modificaciones propuestas serán examinadas por el organismo notificado, que decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos contemplados en el punto 3.2 o si es necesaria una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación contendrá las conclusiones del examen de los cambios y la decisión de evaluación motivada.

4. Control de la documentación técnica.

4.1. Además de la solicitud contemplada en el punto 3, el proveedor presentará una solicitud ante un organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que tenga previsto comercializar o poner en servicio y que esté cubierto por el sistema de gestión de la calidad contemplado en el punto 3.

4.2. La solicitud deberá incluir:

(a) el nombre y la dirección del proveedor;

(b) una declaración escrita de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;

(c) la documentación técnica mencionada en el Anexo IV.

4.3. El organismo notificado examinará la documentación técnica. ***Cuando proceda, y limitado a lo necesario para el desempeño de sus tareas***, se concederá al organismo notificado pleno acceso a los conjuntos de datos de formación***, validación*** y ensayo utilizados, ***incluso, cuando proceda y con sujeción a las salvaguardias de seguridad,*** mediante API u otros medios ***técnicos*** y herramientas ***pertinentes*** que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor aporte más pruebas o realice más ensayos para poder evaluar adecuadamente la conformidad del sistema de IA con los requisitos establecidos en la sección 2 del capítulo III. En caso de que el organismo notificado no esté satisfecho con los ensayos realizados por el proveedor, el propio organismo notificado realizará directamente los ensayos adecuados, según proceda.

4.5. Cuando sea necesario para evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2***, después de que se hayan agotado todos los demás medios razonables para verificar la conformidad y hayan resultado insuficientes,*** y previa solicitud motivada, también se concederá al organismo notificado acceso a los ***modelos de entrenamiento y entrenados*** del sistema de IA***, incluidos sus parámetros pertinentes***. ***Dicho acceso estará sujeto al Derecho de la Unión vigente en materia de protección de la propiedad intelectual y de los secretos comerciales.***

4.6. La decisión del organismo notificado se notificará al proveedor o a su representante autorizado. La notificación incluirá las conclusiones de la evaluación de la documentación técnica y la decisión de evaluación motivada.

Cuando el sistema de IA sea conforme con los requisitos establecidos en el capítulo III, sección 2, el organismo notificado expedirá un certificado de evaluación de la documentación técnica de la Unión.
El certificado indicará el nombre y la dirección del proveedor, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para la identificación del sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente que permita evaluar la conformidad del sistema de IA y, en su caso, controlar el sistema de IA durante su utilización.

En caso de que el sistema de IA no sea conforme con los requisitos establecidos en el capítulo III, sección 2, el organismo notificado se negará a expedir un certificado de evaluación de la documentación técnica de la Unión e informará de ello al solicitante, explicando detalladamente su negativa.

Cuando el sistema de IA no cumpla el requisito relativo a los datos utilizados para entrenarlo, será necesario volver a entrenarlo antes de solicitar una nueva evaluación de la conformidad. En este caso, la decisión de evaluación motivada del organismo notificado por la que se deniegue la expedición del certificado de evaluación de la documentación técnica de la Unión contendrá consideraciones específicas sobre los datos de calidad utilizados para entrenar el sistema de IA, en particular sobre los motivos del incumplimiento.

4.7. El organismo notificado que haya expedido el certificado de evaluación de la documentación técnica de la Unión evaluará cualquier cambio del sistema de IA que pueda afectar a su conformidad con los requisitos o a su finalidad prevista. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios antes mencionados, o si tiene conocimiento de que se van a producir. Los cambios previstos serán evaluados por el organismo notificado, que decidirá si dichos cambios requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden abordarse mediante un suplemento del certificado de evaluación de la documentación técnica de la Unión. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si se aprueban los cambios, expedirá al proveedor un suplemento del certificado de evaluación de la documentación técnica de la Unión.

5. Vigilancia del sistema de gestión de la calidad aprobado.

5.1. El objetivo de la vigilancia efectuada por el organismo notificado mencionado en el punto 3 es cerciorarse de que el proveedor cumple debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de evaluación, el proveedor permitirá al organismo notificado acceder a los locales en los que se lleven a cabo el diseño, el desarrollo y los ensayos de los sistemas de IA. Además, el proveedor compartirá con el organismo notificado toda la información necesaria.

5.3. El organismo notificado efectuará auditorías periódicas para cerciorarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad y facilitará al proveedor un informe de la auditoría. En el contexto de dichas auditorías, el organismo notificado podrá realizar ensayos adicionales de los sistemas de IA para los que se haya expedido un certificado de evaluación de la documentación técnica de la Unión.

ANEXO VIII

Información que debe presentarse en el momento del registro de los sistemas de IA de alto riesgo de conformidad con el artículo 49

Sección A - Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el apartado 1 del artículo 49

Se facilitará la siguiente información, que posteriormente se mantendrá actualizada, en relación con los sistemas de IA de alto riesgo que deban registrarse de conformidad con el ***apartado 1 del*** artículo 49:

1. Nombre, dirección y datos de contacto del proveedor;
2. Cuando la presentación de la información la realice otra persona en nombre del proveedor, el nombre, la dirección y los datos de contacto de dicha persona;
3. El nombre, la dirección y los datos de contacto del representante autorizado, si procede;
4. El nombre comercial del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;
5. Una descripción de la finalidad prevista del sistema de ***IA y de los componentes y funciones que se apoyan a través de este sistema de IA***;
6. ***Descripción básica y concisa de la información utilizada por el sistema (datos, entradas) y su lógica de funcionamiento;***

7. El estado del sistema de IA (en el mercado o en servicio; ya no está en el mercado o en servicio, retirado);

8. El tipo, número y fecha de expiración del certificado expedido por el organismo notificado y el nombre o número de identificación de dicho organismo notificado, en su caso;

9. Una copia escaneada del certificado mencionado en el punto 8, si procede;

10. Todos los Estados miembros en los que el sistema de IA estaba en el mercado, se puso en servicio o se hizo disponible en la Unión;

11. Una copia de la declaración UE de conformidad mencionada en el artículo 47;

12. Instrucciones electrónicas de uso; esta información no se facilitará para los sistemas de IA de alto riesgo en los ámbitos policial o de gestión de la migración, el asilo y el control de fronteras a que se refieren los puntos 1, 6 y 7 del anexo III;

13. Una URL para obtener información adicional (opcional).

Sección B - Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el apartado 2 del artículo 49

En relación con los sistemas de IA que deban registrarse de conformidad con el apartado 2 del artículo 49, se facilitará la siguiente información, que posteriormente se mantendrá actualizada:

1. ***Nombre, dirección y datos de contacto del proveedor;***
2. ***Cuando la presentación de la información la realice otra persona en nombre del proveedor, el nombre, la dirección y los datos de contacto de dicha persona;***
3. ***El nombre, la dirección y los datos de contacto del representante autorizado, si procede;***
4. ***El nombre comercial del sistema de IA y cualquier referencia adicional inequívoca que permita la identificación y trazabilidad del sistema de IA;***
5. ***Descripción de la finalidad prevista del sistema de IA;***
6. ***La condición o condiciones contempladas en el apartado 3 del artículo 6 por las que se considera que el sistema de IA no es de alto riesgo;***
7. ***Breve resumen de los motivos por los que se considera que el sistema de IA no presenta un riesgo elevado en aplicación del procedimiento del apartado 3 del artículo 6;***
8. ***Estado del sistema de IA (en el mercado o en servicio; ya no está en el mercado o en servicio, retirado);***
9. ***Cualquier Estado miembro en el que el sistema de IA se haya comercializado, puesto en servicio o puesto a disposición en la Unión.***

Sección C - Información que deben presentar los implantadores de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 3

Se facilitará la siguiente información, que posteriormente se mantendrá actualizada, en relación con los sistemas de IA de alto riesgo que deban registrarse de conformidad con el artículo 49:

1. ***El nombre, la dirección y los datos de contacto del responsable de la implantación;***
2. ***El nombre, la dirección y los datos de contacto de la persona que presenta la información en nombre del remitente;***
3. ***Un resumen de las conclusiones de la evaluación de impacto sobre los derechos fundamentales realizada de conformidad con el artículo 27;***
4. ***La URL de la entrada del sistema de IA en la base de datos de la UE por su proveedor;***
5. ***Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en*** el artículo 26, apartado 8, ***del presente Reglamento, cuando proceda.***

ANEXO IX

Información que debe presentarse en el momento del registro de los sistemas de IA de alto riesgo enumerados en el anexo III en relación con las pruebas en condiciones reales de conformidad con el artículo 60

Se facilitará la siguiente información, que posteriormente se mantendrá actualizada, en relación con los ensayos en condiciones reales que se registrarán de conformidad con el artículo 60:

1. ***Un número de identificación único para toda la Unión de las pruebas en condiciones reales;***
2. ***El nombre y los datos de contacto del proveedor o posible proveedor y de las personas que participan en las pruebas en condiciones reales;***
3. ***Breve descripción del sistema de IA, su finalidad prevista y otra información necesaria para la identificación del sistema;***
4. ***Resumen de las principales características del plan de pruebas en condiciones reales;***
5. ***Información sobre la suspensión o finalización de las pruebas en condiciones reales.***

ANEXO X

Actos legislativos de la Unión sobre sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia

1. Sistema de Información de Schengen

   (a) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de los nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018, p. 1).

   (b) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de los controles fronterizos, y por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y por el que se modifica y deroga el Reglamento (CE) nº 1987/2006 (DO L 312 de 7.12.2018, p. 14)

   (c) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del espacio Schengen Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal, por la que se modifica y deroga la Decisión 2007/533/JAI del Consejo y por la que se derogan el Reglamento (CE) nº 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

2. Sistema de Información de Visados

(a) Reglamento (UE) 2021/1133 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (UE) n.º 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 y (UE) 2019/818 en lo que respecta al establecimiento de las condiciones de acceso a otros sistemas de información de la UE a efectos del Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 1).

(b) Reglamento (UE) 2021/1134 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (CE) n.º 767/2008, (CE) n.º 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817
y (UE) 2019/1896 del Parlamento Europeo y del Consejo y por la que se derogan las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, con el fin de reformar el Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 11).

3. Eurodac

(a) Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo relativo a la creación del sistema "Eurodac" para la comparación de datos biométricos para la aplicación efectiva del Reglamento (UE) .../... [Reglamento sobre la gestión del asilo y la migración], del Reglamento (UE) .../... [Reglamento sobre reasentamiento] y de la Directiva 2001/55/CE [Directiva sobre protección temporal] para la identificación de un nacional de un tercer país o apátrida en situación irregular y sobre las solicitudes de comparación con los datos de Eurodac por parte de las autoridades policiales de los Estados miembros y Europol con fines policiales, y por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) **2019/818+**.

+ DO: Insértese en el texto el número del Reglamento contenido en el documento PE-CONS 15/24 (2016/0132 (COD)) e insértese el número, la fecha, el título y la referencia del DO de dicho Reglamento en la nota a pie de página.

4. Sistema de entrada/salida

(a) Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo de de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y los datos de denegación de entrada de los nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros y se determinan las condiciones de acceso al SES a efectos policiales, y por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 (DO L 327 de 9.12.2017, p. 20).

5. Sistema Europeo de Información y Autorización de Viajes

(a) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (ETIAS) y se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 (DO L 236 de 19.9.2018, p. 1).

(b) Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con el fin de establecer un Sistema Europeo de Información y Autorización de Viajes (ETIAS) (DO L 236 de 19.9.2018, p. 72).

6. Sistema europeo de información de antecedentes penales sobre nacionales de terceros países y apátridas

(a) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo de 17 de abril de 2019, por el que se establece un sistema centralizado de identificación de los Estados miembros que poseen información sobre condenas penales para nacionales de terceros países y apátridas (ECRIS-TCN) como complemento del sistema de información europeo de antecedentes penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

7. Interoperabilidad

(a) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad entre la UE
sistemas de información en materia de fronteras y visados (DO L 135 de 22.5.2019, p. 27).

(b) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración
(DO L 135 de 22.5.2019, p. 85).

ANEXO XI

Documentación técnica a que se refiere el artículo 53, apartado 1, letra a) ***- documentación técnica para proveedores de modelos de IA de uso general***

Sección 1

Información que deben facilitar todos los proveedores de modelos de IA de uso general

La documentación técnica a que se refiere la letra a) del apartado 1 del artículo 53 ***contendrá como mínimo la siguiente información, en función del tamaño y el perfil de riesgo del modelo:***

1. Una descripción general del modelo de IA de propósito general que incluye:

(a) las tareas que debe realizar el modelo y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

(b) las políticas de uso aceptable aplicables;

(c) la fecha de publicación y los métodos de distribución;

(d) la arquitectura y el número de parámetros;

(e) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;

(f) la licencia.

2. Una descripción detallada de los elementos del modelo a que se refiere el punto 1, e información pertinente del proceso de elaboración, incluidos los siguientes elementos:

(a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para que el modelo de IA de propósito general se integre en los sistemas de IA;

(b) las especificaciones de diseño del modelo y del proceso de formación, incluidas las metodologías y técnicas de formación, las opciones clave de diseño, incluidos los fundamentos y las suposiciones realizadas; para qué se ha diseñado el modelo con el fin de optimizarlo y la relevancia de los distintos parámetros, según proceda;

(c) información sobre los datos utilizados para la formación, las pruebas y la validación, cuando proceda, incluido el tipo y la procedencia de los datos y las metodologías de curación (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y características principales; cómo se obtuvieron y seleccionaron los datos, así como todas las demás medidas para detectar la inadecuación de las fuentes de datos y los métodos para detectar sesgos identificables, cuando proceda;

(d) los recursos informáticos utilizados para entrenar el modelo (por ejemplo, el número de operaciones en coma flotante -FLOPs-), el tiempo de entrenamiento y otros detalles relevantes relacionados con el entrenamiento;

(e) consumo de energía conocido o estimado del modelo.

Por lo que respecta a la letra e), en la que se desconoce el consumo de energía del modelo, el consumo de energía puede basarse en información sobre los recursos informáticos utilizados.

Sección 2

Información adicional que deben facilitar los proveedores de modelos de IA de propósito general con riesgo sistémico

1. Una descripción detallada de las estrategias de evaluación, incluidos los resultados de la evaluación, sobre la base de los protocolos y herramientas de evaluación públicos disponibles o, en su defecto, de otras metodologías de evaluación. Las estrategias de evaluación incluirán criterios de evaluación, métricas y la metodología sobre la identificación de limitaciones.

2. En su caso, una descripción detallada de las medidas aplicadas con el fin de llevar a cabo pruebas adversativas internas y/o externas (por ejemplo, red teaming), adaptaciones de modelos, incluida la alineación y la puesta a punto.

3. En su caso, una descripción detallada de la arquitectura del sistema que explique cómo los componentes de software se construyen o alimentan entre sí y se integran en el procesamiento global.

ANEXO XII

Información sobre transparencia contemplada en el artículo 53, apartado 1, letra b***)***

- documentación técnica para proveedores de modelos de IA de uso general a proveedores posteriores que integren el modelo en su sistema de IA

La información a que se refiere el artículo 53, apartado 1, letra b), contendrá como mínimo lo siguiente:

1. Una descripción general del modelo de IA de propósito general que incluye:

(a) las tareas que debe realizar el modelo y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

(b) las políticas de uso aceptable aplicables;

(c) la fecha de publicación y los métodos de distribución;

(d) el modo en que el modelo interactúa, o puede utilizarse para interactuar, con hardware o software que no forme parte del propio modelo, cuando proceda;

(e) las versiones de los programas informáticos pertinentes relacionados con el uso del modelo de IA de propósito general, en su caso;

(f) la arquitectura y el número de parámetros;

(g) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;

(h) la licencia del modelo.

2. Una descripción de los elementos del modelo y del proceso para su desarrollo, incluyendo:

(a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para que el modelo de IA de propósito general se integre en los sistemas de IA;

(b) la modalidad (por ejemplo, texto, imagen, etc.) y el formato de las entradas y salidas, así como su tamaño máximo (por ejemplo, la longitud de la ventana contextual, etc.);

(c) información sobre los datos utilizados para la formación, las pruebas y la validación, en su caso, incluido el tipo y la procedencia de los datos y las metodologías de conservación.

ANEXO XIII

Criterios para la designación de los modelos de IA de propósito general con riesgo sistémico a que se refiere el artículo 51

Para determinar que un modelo de IA de propósito general tiene capacidades o un impacto equivalentes a los establecidos en el artículo 51, apartado 1, letras a) y b), la Comisión tendrá en cuenta los siguientes criterios:

(a) ***el número de parámetros del modelo;***

(b) ***la calidad o el tamaño del conjunto de datos, por ejemplo, medido a través de tokens;***

(c) ***la cantidad de cálculo utilizada para entrenar el modelo, medida en FLOPs o indicada por una combinación de otras variables como el coste estimado del entrenamiento, el tiempo estimado necesario para el entrenamiento o el consumo de energía estimado para el entrenamiento;***

(d) ***las modalidades de entrada y salida del modelo, como texto a texto (grandes modelos lingüísticos), texto a imagen, multimodalidad, y los umbrales del estado de la técnica para determinar las capacidades de alto impacto para cada modalidad, y el tipo específico de entradas y salidas (por ejemplo, secuencias biológicas);***

(e) ***los puntos de referencia y las evaluaciones de las capacidades del modelo, incluyendo la consideración del número de tareas sin formación adicional, la adaptabilidad para aprender tareas nuevas y distintas, su grado de autonomía y escalabilidad, las herramientas a las que tiene acceso;***

(f) ***si tiene un gran impacto en el mercado interior debido a su alcance, que se presumirá cuando se haya puesto a disposición de al menos 10 000 usuarios empresariales registrados establecidos en la Unión;***

(g) ***el número de usuarios finales registrados.***