Consejo de la Unión Europea

Bruselas, 25 de noviembre de 2022
(OR. en)

14954/22

Expediente interinstitucional: 2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

NOTA

De:	Comité de Representantes Permanentes (1.ª parte)
A:	Consejo
N.º doc. prec.:	14336/22
N.° doc. Ción.:	8115/21
Asunto:	Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión - Orientación general

I. INTRODUCCIÓN

1. La Comisión adoptó la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (**Reglamento de Inteligencia Artificial**) el 21 de abril de 2021.

2. La propuesta de la Comisión tiene por objeto garantizar que los sistemas de inteligencia artificial (IA) comercializados en el mercado de la Unión y utilizados en ella sean seguros y respeten la legislación vigente relativa a los derechos fundamentales y los valores de la Unión, garantizar la seguridad jurídica para facilitar la inversión y la innovación en IA y mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y seguridad, así como facilitar el desarrollo de un mercado único de aplicaciones de inteligencia artificial que sean legales, seguras y fiables y evitar la fragmentación del mercado.

II. TRABAJOS EN OTRAS INSTITUCIONES

3. En el Parlamento Europeo, dirige los debates la Comisión de Mercado Interior y Protección del Consumidor (IMCO; ponente: Brando Benifei, S&D, Italia) y la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE; ponente: Dragos Tudorache, Renew, Rumanía), en el marco de un procedimiento de comisiones conjuntas. También participan en la labor legislativa la Comisión de Asuntos Jurídicos (JURI), la Comisión de Industria, Investigación y Energía (ITRE) y la Comisión de Cultura y Educación (CULT) con competencias compartidas o exclusivas. Los dos coponentes presentaron su proyecto de informe en abril de 2022 y está previsto que la votación sobre el informe conjunto de las comisiones IMCO y LIBE tenga lugar en el primer trimestre de 2023.

4. El Comité Económico y Social Europeo emitió su dictamen sobre la propuesta el 22 de septiembre de 2021 y el Comité Europeo de las Regiones emitió el suyo el 2 de diciembre de 2021.

5. El 18 de junio de 2021, el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) emitieron un dictamen conjunto sobre la propuesta.

6. El Banco Central Europeo (BCE) emitió su dictamen el 29 de diciembre de 2021 y lo presentó al Grupo «Telecomunicaciones y Sociedad de la Información» (Grupo TELECOM), el 10 de febrero de 2022.

III. SITUACIÓN DE LOS TRABAJOS EN EL CONSEJO

1. En el Consejo, el estudio de la propuesta se ha llevado a cabo en el Grupo «TELECOM». El Grupo «TELECOM» empezó a debatir la propuesta durante la Presidencia portuguesa, en varias reuniones y talleres celebrados entre abril y junio de 2021. Se siguió trabajando en la propuesta durante la Presidencia eslovena, que elaboró la primera propuesta transaccional parcial, que abarcaba los **artículos 1 a 7** y los **anexos I a III**. Además, la Presidencia eslovena convocó un Consejo informal de ministros de Telecomunicaciones, de medio día de duración, dedicado exclusivamente a la propuesta de Reglamento de Inteligencia Artificial, en el que los ministros confirmaron su acuerdo con la adopción de un planteamiento horizontal y centrado en el ser humano en relación con la reglamentación de la IA. La Presidencia francesa siguió examinando el expediente y, al final de su mandato, reformuló las partes restantes del texto (los **artículos 8 a 85** y los **anexos IV a IX**) y presentó la primera propuesta transaccional consolidada sobre el Reglamento de Inteligencia Artificial el 17 de junio de 2022.

2. El 5 de julio de 2022, la Presidencia checa mantuvo un debate de orientación en el Grupo «TELECOM» en torno al documento de opciones estratégicas, cuyos resultados sirvieron para la elaboración del **segundo texto transaccional**. A partir de los comentarios de las delegaciones sobre este segundo texto transaccional, la Presidencia checa elaboró el **tercer texto transaccional**, que se presentó y debatió en el Grupo «TELECOM» los días 22 y 29 de septiembre de 2022. Tras estos debates, se pidió a las delegaciones que presentaran nuevas observaciones escritas, que la Presidencia checa utilizó para elaborar la **cuarta propuesta transaccional**. A partir de los debates sobre la cuarta propuesta transaccional mantenidos en el Grupo «TELECOM» los días 25 de octubre y 8 de noviembre de 2022, y teniendo en cuenta las últimas observaciones escritas de los Estados miembros, la Presidencia checa ha elaborado la **versión definitiva del texto transaccional**, que se adjunta en el anexo. El 18 de noviembre, el Coreper estudió la propuesta transaccional y **acordó por unanimidad remitirla sin cambios al Consejo TTE (Telecomunicaciones), con vistas a la adopción de una orientación general** en su sesión del 6 de diciembre de 2022.

IV. PRINCIPALES ELEMENTOS DE LA PROPUESTA TRANSACCIONAL

1. Definición de un sistema de IA, prácticas de IA prohibidas, lista de supuestos de utilización de sistemas de IA de alto riesgo en el anexo III y clasificación de sistemas de IA como de alto riesgo

1.1 Para garantizar que la definición de los sistemas de IA proporcione criterios suficientemente claros para distinguirlos de otros sistemas de *software* más clásicos, el texto transaccional restringe la definición del **artículo 3, apartado 1**, a los sistemas desarrollados a través de estrategias de aprendizaje automático y estrategias basadas en la lógica y el conocimiento.

1.2 Por lo que respecta a la delegación de poderes a la Comisión en relación con la actualización de la definición de los sistemas de IA, se ha suprimido el **anexo I** y los correspondientes poderes de la Comisión para la adopción de actos delegados para actualizarlo. En su lugar, se han añadido los **considerandos 6 *bis* y 6 *ter*** para aclarar los conceptos de «estrategia de aprendizaje automático» y «estrategias basadas en la lógica y el conocimiento». Para garantizar que el Reglamento de Inteligencia Artificial sea flexible y pueda adaptarse a las transformaciones futuras, se ha añadido, en el **artículo 4**, la posibilidad de adoptar actos de ejecución para especificar y actualizar las técnicas de las estrategias de aprendizaje automático y de las estrategias basadas en la lógica y el conocimiento.

1.3 En lo que respecta a las prácticas de IA prohibidas, el **artículo 5** del texto transaccional amplía a los agentes privados la prohibición de utilizar la IA con fines de puntuación ciudadana. Además, la disposición por la que se prohíbe el uso de sistemas de IA que aprovechan las vulnerabilidades de grupos específicos de personas ahora incluye también a las personas vulnerables por su situación social o económica. Por lo que respecta a la prohibición relativa al uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público por parte de las autoridades encargadas de la aplicación de la ley, el texto transaccional enumera los objetivos para cuya consecución se considera que dicho uso es estrictamente necesario con fines de aplicación de la ley y a qué autoridades encargadas de la aplicación de la ley se les debe, por tanto, permitir excepcionalmente el uso de dichos sistemas.

1.4 Por lo que se refiere a la lista de supuestos de utilización de la IA de alto riesgo que figura en el **anexo III**, se han suprimido tres de ellos (la detección de ultrafalsificaciones por parte de las autoridades encargadas de la aplicación de la ley, la realización de análisis penales y la comprobación de la autenticidad de los documentos de viaje), se han añadido dos nuevos (las infraestructuras digitales críticas y los seguros de vida y salud) y otros se han matizado. Por otra parte, se ha modificado el **artículo 7, apartado 1**, para prever la posibilidad no solo de añadir a la lista supuestos de uso de alto riesgo mediante actos delegados, sino también de suprimirlos. A fin de garantizar una protección adecuada de los derechos fundamentales en caso de que se produzcan tales supresiones, se han añadido disposiciones adicionales en el **artículo 7, apartado 3**, en las que se especifican las condiciones que deben cumplirse antes de que pueda adoptarse un acto delegado.

1.5 En cuanto a la clasificación de los sistemas de IA como de alto riesgo, la propuesta transaccional incluye ahora una serie de criterios de clasificación horizontales que se añaden a la clasificación de sistemas de alto riesgo que figura en el **anexo III**, con el fin de garantizar que no se incluyan en la clasificación de sistemas de alto riesgo sistemas de IA que probablemente no provocarán violaciones graves de los derechos fundamentales u otros riesgos significativos. Más concretamente, el artículo 6, apartado 3, contiene nuevas disposiciones que establecen que, al clasificar un sistema de IA como de alto riesgo, también debe tenerse en cuenta la relevancia de la información de salida del sistema de IA respecto de la acción o decisión que se vaya a adoptar. Para evaluar la relevancia de la información de salida del sistema de IA se debe determinar si dicha información es meramente accesoria respecto de la acción o decisión que vaya a adoptarse.

2. Requisitos de los sistemas de IA de alto riesgo y responsabilidades de diversos agentes de la cadena de valor de la IA

2.1 Se han aclarado y precisado muchos de los requisitos de los sistemas de IA de alto riesgo que se establecen en el **título III, capítulo 2**, de la propuesta, de manera que sean más viables desde el punto de vista técnico y supongan una carga menor para las partes interesadas, por ejemplo, en lo que respecta a la calidad de los datos o a la documentación técnica que deben elaborar las pymes para demostrar que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos.

2.2 Dado que los sistemas de IA se desarrollan y distribuyen a través de cadenas de valor complejas, el texto transaccional incluye varios cambios que añaden claridad a la asignación de responsabilidades y funciones. Así, por ejemplo, se han añadido algunas disposiciones adicionales en los **artículos 13 y 14** que permiten una cooperación más eficaz entre los proveedores y los usuarios. El texto transaccional también pretende aclarar la relación entre las obligaciones establecidas en virtud del Reglamento de Inteligencia Artificial y las obligaciones ya vigentes en virtud de otros actos legislativos, como la legislación pertinente de la Unión en materia de protección de datos o la legislación sectorial, también en lo que respecta al sector de los servicios financieros. Además, el nuevo **artículo 23** ***bis*** define con mayor claridad los supuestos en los que otros agentes de la cadena de valor están obligados a asumir las responsabilidades del proveedor.

3. **Sistemas de IA de uso general**

3.1 Se ha añadido un nuevo **título I** ***BIS*** para reflejar aquellas situaciones en las que los sistemas de IA pueden utilizarse con muchos fines diferentes (IA de uso general) y en las que pueden darse circunstancias en las que la tecnología de IA de uso general se integre en otro sistema que puede convertirse en un sistema de alto riesgo. El texto transaccional especifica en el artículo **4** ***ter*****, apartado 1**, que determinados requisitos de los sistemas de IA de alto riesgo también se podrían aplicar a los sistemas de IA de uso general. No obstante, estos requisitos no se aplicarían directamente, sino que sería necesario adoptar un acto de ejecución que especificara cómo deben aplicarse en relación con los sistemas de IA de uso general. Dicho acto de ejecución se basará en una consulta y una evaluación de impacto detallada y tendrá en cuenta las características específicas de estos sistemas y la correspondiente cadena de valor, la viabilidad técnica y la evolución tecnológica y del mercado. La utilización de un acto de ejecución garantiza la participación adecuada de los Estados miembros, que tendrán la última palabra sobre cómo se aplicarán los requisitos en este contexto.

3.2 Además, el texto transaccional del **artículo 4** ***ter*****, apartado 5**, también prevé la posibilidad de adoptar actos de ejecución adicionales para definir las modalidades de cooperación entre los proveedores de sistemas de IA de uso general y otros proveedores que tengan la intención de poner en servicio o introducir dichos sistemas en el mercado de la Unión como sistemas de IA de alto riesgo, en particular en lo que respecta al suministro de información.

4. **Aclaración del ámbito de aplicación de la propuesta de Reglamento de Inteligencia Artificial y disposiciones relativas a las autoridades encargadas de la aplicación de la ley**

4.1 En el **artículo 2** se dispone expresamente que se excluyen del ámbito de aplicación del Reglamento de Inteligencia Artificial las actividades militares o las relacionadas con la defensa y la seguridad nacional. Asimismo, se ha aclarado que el Reglamento de Inteligencia Artificial no debe aplicarse a los sistemas de IA, incluida su información de salida, que se utilicen únicamente con fines de investigación y desarrollo ni a las obligaciones de las personas que utilicen la IA con fines no profesionales, que quedarían fuera del ámbito de aplicación del Reglamento de Inteligencia Artificial, excepto por lo que respecta a las obligaciones de transparencia.

4.2 Con el fin de tener en cuenta las particularidades de las distintas autoridades encargadas de la aplicación de la ley, se han hecho una serie de modificaciones a las disposiciones relativas al uso de sistemas de IA con fines de aplicación de la ley. En particular, se han pulido algunas de las definiciones del **artículo 3** relacionadas con esta cuestión, como las de los términos «sistema de identificación biométrica remota» y «sistema de identificación biométrica remota "en tiempo real"», para aclarar qué situaciones entrarían en el ámbito de aplicación de la prohibición correspondiente y constituirían supuestos de uso de alto riesgo y qué situaciones no. La propuesta transaccional también contiene otras modificaciones que, con las garantías oportunas, tienen por objeto garantizar un nivel adecuado de flexibilidad en el uso de sistemas de IA de alto riesgo por parte de las autoridades encargadas de la aplicación de la ley o reflexionar sobre la necesidad de respetar la confidencialidad de los datos operativos delicados relativos a sus actividades.

5. **Evaluaciones de conformidad, marco de gobernanza, vigilancia del mercado, aplicación y sanciones**

5.1 Con el fin de simplificar el marco de cumplimiento del Reglamento de Inteligencia Artificial, el texto transaccional contiene una serie de aclaraciones y simplificaciones de las disposiciones sobre los procedimientos de evaluación de la conformidad. También se han aclarado y simplificado las disposiciones relativas a la vigilancia del mercado para que sean más eficaces y fáciles de aplicar, teniendo en cuenta la necesidad de adoptar una solución proporcionada en este sentido. Además, se ha revisado exhaustivamente el **artículo 41** para limitar la discrecionalidad de la Comisión con respecto a la adopción de actos de ejecución que establezcan especificaciones técnicas comunes para los requisitos aplicables a los sistemas de IA de alto riesgo y los sistemas de IA de uso general.

5.2 El texto transaccional también modifica sustancialmente las disposiciones relativas al Comité de IA (en lo sucesivo, «el Comité»), con el fin de atribuirle una mayor autonomía y reforzar su papel en la arquitectura de gobernanza del Reglamento de Inteligencia Artificial. En este sentido, se han revisado los **artículos 56 y 58** con el fin de reforzar el papel del Comité, de manera que esté en mejores condiciones para prestar apoyo a los Estados miembros en la aplicación y el cumplimiento del Reglamento de Inteligencia Artificial. Más concretamente, se han ampliado las funciones del Comité y se ha precisado su composición. Con el fin de garantizar la participación de las partes interesadas en todas las cuestiones relacionadas con la aplicación del Reglamento de Inteligencia Artificial, incluida la elaboración de actos de ejecución y delegados, se ha añadido el requisito de que el Comité cree un subgrupo permanente que sirva de plataforma para un amplio abanico de partes interesadas. También deben crearse otros dos subgrupos permanentes, uno para las autoridades de vigilancia del mercado y otro para las autoridades notificantes, con el fin de reforzar la coherencia de la gobernanza y la aplicación del Reglamento de Inteligencia Artificial en toda la Unión.

5.3 Para seguir mejorando el marco de gobernanza, el texto transaccional incluye los nuevos **artículos 68 *bis* y 68 *ter***. El **artículo 68 *bis*** establece el requisito de que la Comisión designe una o varias instalaciones de ensayo de la Unión en el ámbito de la inteligencia artificial para que proporcionen asesoramiento técnico o científico independiente a petición del Comité o de las autoridades de vigilancia del mercado, mientras que el **artículo 68 *ter*** impone a la Comisión la obligación de crear un grupo central de expertos independientes para respaldar las actividades de aplicación exigidas en virtud del Reglamento de Inteligencia Artificial. Por último, se añade un nuevo **artículo 58 *bis*** que establece la obligación de la Comisión de elaborar orientaciones sobre la aplicación del Reglamento de Inteligencia Artificial.

5.4 Por lo que se refiere a las sanciones por el incumplimiento de las disposiciones del Reglamento de Inteligencia Artificial, el **artículo 71** del texto transaccional establece límites más proporcionados al importe de las multas administrativas que pueden imponerse a las pymes y las empresas emergentes. Además, en el **artículo 71, apartado 6,** se han añadido cuatro criterios más para decidir el importe de las multas administrativas con el fin de proteger en aún mayor medida su proporcionalidad global.

6. **Transparencia y otras disposiciones a favor de las personas afectadas**

6.1 La propuesta transaccional incluye varios cambios para reforzar la transparencia en relación con el uso de sistemas de IA de alto riesgo. Concretamente, se ha actualizado el **artículo 51** para indicar que determinados usuarios de sistemas de IA de alto riesgo que sean autoridades públicas, órganos u organismos también estarán obligados a registrarse en la base de datos de la UE de sistemas de IA de alto riego que se enumeran en el anexo III. Asimismo, el **nuevo apartado 2 *bis* del artículo 52** hace hincapié en la obligación de los usuarios de un sistema de reconocimiento de emociones de informar a las personas físicas a las que se exponga a dicho sistema.

6.2 La propuesta transaccional también deja claro en el **nuevo apartado 11 del artículo 63** que una persona física o jurídica que tenga motivos para considerar que se ha producido una infracción de lo dispuesto en el Reglamento de Inteligencia Artificial puede presentar una reclamación ante la correspondiente autoridad de vigilancia del mercado y esperar que dicha reclamación se tramite de conformidad con los procedimientos específicos de dicha autoridad.

7. **Medidas de apoyo a la innovación**

7.1 Con el objetivo de crear un marco jurídico más favorable a la innovación y con el fin de promover un aprendizaje reglamentario basado en pruebas, las disposiciones relativas a las medidas de apoyo a la innovación del **artículo 53** se han modificado sustancialmente en el texto transaccional. En particular, se ha aclarado que los espacios controlados de pruebas de IA, cuya finalidad es ofrecer un entorno controlado para desarrollar, probar y validar sistemas innovadores de IA bajo la supervisión y orientación directas de las autoridades nacionales competentes, también deben permitir probar sistemas innovadores de IA en condiciones reales. Además, se han añadido nuevas disposiciones en los **artículos 54 *bis* y 54 *ter*** que permiten probar los sistemas de IA en condiciones reales no supervisadas, siempre que se den determinadas circunstancias y se ofrezcan determinadas garantías. En ambos casos, el texto transaccional aclara cómo deben interpretarse las nuevas normas en relación con otras normativas sectoriales vigentes sobre los espacios controlados de pruebas.

7.2 Por último, con el fin de aliviar la carga administrativa de las empresas más pequeñas, el texto transaccional incluye en el artículo 55 una lista de las acciones que debe emprender la Comisión para ayudar a dichos operadores, y en el **artículo 55 *bis*** prevé algunas excepciones limitadas y claramente especificadas.

V. CONCLUSIÓN

1. A la vista de lo anterior, se ruega al Consejo que:
   - examine el texto transaccional que figura en el anexo de la presente nota;
   - confirme la orientación general sobre la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) en la sesión del Consejo TTE (Telecomunicaciones) del 6 de diciembre de 2022.

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (REGLAMENTO DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN

(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 Comité de las Regiones[2],

Visto el dictamen del Banco Central Europeo[3],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

[1] DO C […], […], p. […].
[2] DO C […], […], p. […].
[3] Referencia del dictamen del BCE.

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interno mediante el establecimiento de un marco jurídico uniforme, en particular en lo que respecta al desarrollo, la comercialización y la utilización de la inteligencia artificial de conformidad con los valores de la Unión. El presente Reglamento persigue varios fines imperiosos de interés general, tales como asegurar un nivel elevado de protección de la salud, la seguridad y los derechos humanos, y garantiza la libre circulación transfronteriza de bienes y servicios basados en la inteligencia artificial (IA), con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de inteligencia artificial, a menos que el presente Reglamento lo autorice expresamente.

(2) Los sistemas de inteligencia artificial («sistemas de IA») pueden emplearse con facilidad en múltiples sectores de la economía y la sociedad, también a escala transfronteriza, y circular por toda la Unión. Algunos Estados miembros ya han estudiado la posibilidad de adoptar normas nacionales destinadas a garantizar que la inteligencia artificial sea segura y se desarrolle y utilice de conformidad con las obligaciones relativas a los derechos fundamentales. La existencia de distintas normas nacionales puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan, importan o utilizan sistemas de IA. Por lo tanto, es preciso garantizar un nivel elevado y coherente de protección en toda la Unión y evitar las divergencias que obstaculizan la libre circulación en el mercado interior de los sistemas de IA y los productos y servicios conexos mediante el establecimiento de obligaciones uniformes para todos los operadores y la garantía de una protección uniforme de los fines imperiosos de interés general 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 para la protección de las personas en relación con el tratamiento de datos personales que restringen el uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, resulta adecuado basar este Reglamento, en lo que atañe a dichas normas específicas, en el artículo 16 del TFUE. A la luz de dichas normas específicas y de la invocación del artículo 16 del TFUE, conviene consultar al Comité Europeo de Protección de Datos.

(3) La inteligencia artificial es un conjunto de tecnologías de rápida evolución que puede generar un amplio abanico de beneficios económicos y sociales en todos los sectores y actividades sociales. El uso de la inteligencia artificial puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la educación y la formación, la administración de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, y la mitigación del cambio climático y la adaptación a él, entre otros, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones.

(4) Al mismo tiempo, dependiendo de las circunstancias de su aplicación y utilización concretas, la inteligencia artificial puede generar riesgos y menoscabar los intereses públicos y los derechos que protege el Derecho de la Unión, de manera tangible o intangible.

(5) Por este motivo, se necesita un marco jurídico de la Unión que defina unas normas armonizadas en materia de inteligencia artificial orientadas a impulsar el desarrollo, la utilización y la adopción en el mercado interior de la inteligencia artificial y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad, y de los derechos fundamentales reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado y la puesta en servicio de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de la libre circulación de bienes y servicios. Al establecer tales normas, el presente Reglamento, que se basa en la labor del grupo de expertos de alto nivel sobre la IA reflejada en las Directrices para una IA fiable en la UE, respalda el objetivo de la Unión de ser un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética, como indicó el Consejo Europeo[4], y garantiza la protección de los principios éticos, como solicitó específicamente el Parlamento Europeo[5].

---

[4] Consejo Europeo, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones, EUCO 13/20, 2020, p. 6.

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

(5 *bis*) Las normas armonizadas sobre la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA que se establecen en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con el planteamiento del nuevo marco legislativo, deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo y seguridad de los productos, al que complementa el presente Reglamento. En consecuencia, permanecerán inalterados y seguirán siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA, en particular en lo que respecta a la reparación de los posibles daños de conformidad con la 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. Además, el presente Reglamento tiene por objeto reforzar la eficacia de tales derechos y vías de recurso vigentes mediante el establecimiento de requisitos y obligaciones específicos, en particular en lo que respecta a la transparencia, la documentación técnica y el registro de los sistemas de IA. Asimismo, las obligaciones impuestas a los distintos operadores que participan en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio de la legislación nacional que, siendo conforme al Derecho de la Unión, que tenga por efecto limitar el uso de determinados sistemas de IA cuando dicha legislación no entre en el ámbito de aplicación del presente Reglamento o persiga objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Así, por ejemplo, el presente Reglamento no debe afectar a la legislación laboral nacional ni a la legislación en materia de protección de menores (es decir, de personas de menos de 18 años), habida cuenta de la Observación general n.º 25 de las Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital, en la medida en que no son específicas a los sistemas de IA y persiguen otros objetivos legítimos de interés público.

(6) Resulta necesario definir con claridad la noción de sistema de IA para ofrecer seguridad jurídica, al mismo tiempo que se proporciona la flexibilidad necesaria para adaptarse a los futuros avances tecnológicos. Dicha definición debe basarse en las principales características funcionales de la inteligencia artificial, como su capacidad de aprendizaje, de razonamiento o de modelización, diferenciándola de otros sistemas de software y planteamientos de programación más sencillos. En particular, a los efectos del presente Reglamento, los sistemas de IA deben tener la capacidad de inferir, a partir de datos e información generados por máquinas o por seres humanos, la manera de alcanzar una serie de objetivos definidos por seres humanos, utilizando para ello estrategias de aprendizaje automático o estrategias basadas en la lógica y el conocimiento, y de generar información de salida, como contenidos para sistemas de inteligencia artificial generativa (por ejemplo, texto, vídeo o imágenes), predicciones, recomendaciones o decisiones que influyan en el entorno con el que interactúa el sistema, ya sea en una dimensión física o digital. Los sistemas que utilizan reglas definidas únicamente por personas físicas para ejecutar operaciones de manera automática no deben considerarse sistemas de IA. Los sistemas de IA pueden diseñarse para operar con distintos niveles de autonomía y utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente de él (integrado) o tiene una funcionalidad en el producto sin formar parte de él (no integrado). El concepto de la autonomía de un sistema de IA se refiere a la medida en que dicho sistema puede funcionar sin intervención humana.

(6 *bis*) Las estrategias de aprendizaje automático se centran en el desarrollo de sistemas capaces de aprender y hacer inferencias a partir de datos para resolver un problema de aplicación, sin estar expresamente programados con una serie de instrucciones que abarquen todos los pasos desde la entrada hasta la salida. El aprendizaje se refiere al proceso informático de optimizar, a partir de los datos, los parámetros del modelo, que es un constructo matemático que genera una información de salida a partir de los datos de entrada. Los problemas que aborda el aprendizaje automático suelen incluir tareas en las que las otras estrategias fallan, ya sea porque el problema no está adecuadamente formalizado o porque su resolución es inabordable con estrategias sin aprendizaje. Las estrategias de aprendizaje automático incluyen, por ejemplo, el aprendizaje supervisado, el aprendizaje no supervisado y el aprendizaje por refuerzo, y utilizan diversos métodos, entre los que se incluyen el aprendizaje profundo con redes neuronales, las técnicas estadísticas de aprendizaje e inferencia (como, por ejemplo, la regresión logística o la estimación bayesiana) y los métodos de búsqueda y optimización.

(6 *ter*) Las estrategias basadas en la lógica y el conocimiento tienen por objeto el desarrollo de sistemas con capacidad de razonamiento lógico a partir de conocimientos para la resolución de un problema de aplicación. Estos sistemas suelen incluir una base de conocimientos y un motor de inferencia, que genera información de salida haciendo razonamientos a partir de la base de conocimientos. La base de conocimientos, normalmente codificada por expertos humanos, representa entidades y relaciones lógicas que son pertinentes para el problema de aplicación, usando para ello formalismos basados en normas, ontologías y gráficos de conocimientos. El motor de inferencia interactúa con la base de conocimientos y extrae de ella información nueva a través de operaciones como la clasificación, la búsqueda, el emparejamiento o el encadenamiento. Las estrategias basadas en la lógica y el conocimiento incluyen, por ejemplo, la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, el razonamiento (simbólico), los sistemas expertos y los métodos de búsqueda y optimización.

(6 *quater*) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento por lo que respecta a las estrategias de aprendizaje automático y las estrategias basadas en la lógica y el conocimiento, deben conferirse a la Comisión competencias de ejecución.

(6 *quinquies*) El concepto de «usuario» en el sentido de lo dispuesto en el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad pública, órgano u organismo de otra índole, que utilice un sistema de IA o bajo cuya autoridad se utilice el sistema. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del usuario.

(7) El concepto de «datos biométricos» empleado en el presente Reglamento debe interpretarse en consonancia con el concepto de «datos biométricos» definido en el artículo 4, punto 14, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[6]; en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[7], y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[8].

[6] 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).

[7] 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 esos 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).

[8] 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 parte de 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 dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva sobre Protección de Datos en el Ámbito Penal) (DO L 119 de 4.5.2016, p. 89).

(8) El concepto de «sistema de identificación biométrica remota» que se utiliza en el presente Reglamento debe definirse de manera funcional como un sistema de IA destinado a identificar a personas físicas, generalmente a distancia, sin su participación activa, comparando sus datos biométricos con los que figuren en un repositorio de datos de referencia, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Estos sistemas de identificación biométrica remota suelen utilizarse para detectar (o escanear) a varias personas o su comportamiento de forma simultánea, a fin de simplificar significativamente la identificación de varias personas sin su participación activa. Quedan excluidos de la definición los sistemas de verificación o autenticación cuyo único propósito es confirmar que una determinada persona física es la persona que afirma ser y los sistemas que se utilizan para confirmar la identidad de una persona física con el único fin de tener acceso a un servicio, un dispositivo o un local. La exclusión se justifica por el hecho de que tales sistemas probablemente tengan una repercusión menor en los derechos fundamentales de las personas físicas que los sistemas de identificación biométrica remota que pueden utilizarse para el tratamiento de los datos biométricos de un gran número de personas. En el caso de los sistemas «en tiempo real», la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una demora significativa. En este sentido, no debe existir la posibilidad de eludir las normas contempladas en el presente Reglamento en relación con el uso «en tiempo real» de los sistemas de IA en cuestión generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de material «en directo» o «casi en directo», como grabaciones de vídeo generadas por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» ya se han recabado los datos biométricos y la comparación e identificación se producen con una demora significativa. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, que se han generado antes de aplicar el sistema a las personas físicas en cuestión.

(9) A los efectos del presente Reglamento, debe entenderse por «espacio de acceso público» cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de la actividad para la que pueda utilizarse el lugar, ya sean actividades comerciales (tiendas, restaurantes, cafeterías), de prestación de servicios (bancos, actividades profesionales, hostelería), deportivas (por ejemplo, piscinas, gimnasios, estadios), de transporte (estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte), de entretenimiento (cines, teatros, museos, salas de conciertos, salas de conferencias), de ocio o de otro tipo (carreteras y plazas públicas, parques, bosques, parques infantiles). Asimismo, debe considerarse que un lugar es de acceso público si, con independencia de la posibilidad de imponer restricciones de capacidad o de seguridad, el acceso está sujeto a determinadas condiciones previas, que puede satisfacer un número indeterminado de personas, por ejemplo, adquiriendo una entrada o un título de transporte, registrándose previamente o teniendo una determinada edad. Por el contrario, un lugar no debe considerarse de acceso público si únicamente pueden acceder a él determinadas personas físicas definidas, ya sea en virtud del Derecho de la Unión o del Derecho nacional directamente relacionado con la seguridad pública o en virtud de una clara manifestación de voluntad de la persona que ejerza la autoridad pertinente en dicho lugar. La posibilidad real de acceso (por ejemplo, una puerta no cerrada con llave o una verja abierta) no implica por sí sola que el lugar sea de acceso público si hay indicios o circunstancias que sugieran lo contrario (por ejemplo, señales que prohíban o restrinjan el acceso). Los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que accedan los empleados y proveedores de servicios pertinentes, no son lugares de acceso público. No se incluyen en los espacios de acceso público las prisiones o las zonas de control fronterizo. Algunos espacios pueden constar tanto de zonas que no son de acceso público como de zonas de acceso público, como el vestíbulo de un edificio residencial privado por el que se accede a una consulta médica o un aeropuerto. Tampoco cubre los espacios en línea, ya que no son espacios físicos. No obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta.

(10) Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, con independencia de si están establecidos en la Unión o en un tercer país, y a los usuarios de sistemas de IA establecidos en la Unión.

(11) Debido a su carácter digital, algunos sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento aunque no se introduzcan en el mercado, se pongan en servicio ni se utilicen en la Unión. Tal es el caso, por ejemplo, de un operador establecido en la Unión que contrate determinados servicios a otro operador establecido fuera de la Unión en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo. En dichas circunstancias, el sistema de IA usado por el operador de fuera de la Unión podría tratar datos recabados legalmente en la UE y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión la información de salida generada por dicho sistema de IA a raíz de su tratamiento, sin que el sistema de IA en cuestión se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar la elusión de este Reglamento y asegurar la protección efectiva de las personas físicas ubicadas en la Unión, el presente Reglamento también debe aplicarse a los proveedores y usuarios de sistemas de IA establecidos en un tercer país, en la medida en que la información de salida generada por dichos sistemas se utilice en la Unión. No obstante, con el objetivo de tener en cuenta los acuerdos existentes y las necesidades especiales de cooperación futura con socios extranjeros con los que se intercambian información y pruebas, el presente Reglamento no debe aplicarse a las autoridades públicas de un tercer país ni a las organizaciones internacionales cuando actúen en el marco de acuerdos internacionales celebrados a escala nacional o europea con fines de cooperación policial y judicial con la Unión o sus Estados miembros. Dichos acuerdos se han celebrado bilateralmente entre los Estados miembros y terceros países o entre la Unión Europea, Europol y otros organismos de la UE y terceros países y organizaciones internacionales. Las autoridades de los Estados miembros y las instituciones, órganos y organismos de la Unión que sean destinatarias de dicha información de salida y que la utilicen siguen siendo responsables de garantizar que su utilización de la información está en consonancia con el Derecho de la Unión. Cuando, en el futuro, dichos acuerdos internacionales se revisen o se celebren otros nuevos las partes contratantes deben hacer todo lo posible por que dichos acuerdos se ajusten a los requisitos del presente Reglamento.

(12) El presente Reglamento debe aplicarse igualmente a las instituciones, órganos y organismos de la Unión cuando actúen como proveedores o usuarios de un sistema de IA.

(-12 *bis*) En caso de que, y en la medida en que, los sistemas de IA se introduzcan en el mercado, se pongan en servicio o se utilicen con o sin modificación con fines militares, de defensa o de seguridad nacional, deben excluirse del ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades, por ejemplo, con independencia de que se trate de una entidad pública o de una entidad privada. Por lo que respecta a los fines militares y de defensa, dicha exclusión está justificada 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 política común de defensa de la Unión contempladas en el título V, capítulo 2, del Tratado de la Unión Europea (TUE) y sujetas al Derecho internacional público que, por lo tanto, es 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 está justificada 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 por las normas nacionales específicas aplicables a dichas actividades. No obstante, si un sistema de IA desarrollado, introducido en el mercado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utilizara fuera de estos ámbitos temporal o permanentemente con otros fines (por ejemplo, con fines civiles o humanitarios, de aplicación de la ley o de seguridad pública), entraría en el ámbito de aplicación del presente Reglamento. En tal caso, la entidad que utilice el sistema con fines que no sean militares, de defensa o de seguridad nacional debe garantizar que el sistema cumple lo dispuesto en el presente Reglamento, a menos que el sistema ya lo haga. Los sistemas de IA introducidos en el mercado o puestos en servicio para un fin excluido (es decir, militar, de defensa o de seguridad nacional) y uno o varios fines no excluidos (por ejemplo, fines civiles, de aplicación de la ley, etc.) entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento del presente Reglamento. En esos 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 llevan a cabo actividades militares, de defensa y de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades, utilicen sistemas de IA con fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento. Un sistema de IA introducido en el mercado con fines civiles o de aplicación de la ley 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 esas actividades.

(12 *bis*) El presente Reglamento debe interpretarse sin perjuicio de las disposiciones de la Directiva 2000/31/CE del Parlamento Europeo y el Consejo (en su versión modificada por la Ley de Servicios Digitales) relativas a la responsabilidad de los prestadores de servicios intermediarios.

(12 *ter*) El presente Reglamento no debe socavar la actividad de investigación y desarrollo, y debe respetar la libertad de la ciencia. Por lo tanto, es necesario excluir de su ámbito de aplicación los sistemas de IA específicamente desarrollados y puestos en servicio con la investigación y el desarrollo científicos como única finalidad y garantizar que el Reglamento no afecte a la actividad de investigación y desarrollo científicos en relación con los sistemas de IA. Por lo que se refiere a la actividad de investigación orientada a los productos que llevan a cabo los proveedores, tampoco deben aplicarse las disposiciones del presente Reglamento. Esto 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 presente Reglamento se introduzca en el mercado o se ponga en servicio como resultado de dichas actividad de investigación y desarrollo, así como de la aplicación de disposiciones sobre espacios controlados de pruebas y ensayos en condiciones reales. Además, sin perjuicio de lo anterior en relación con los sistemas de IA específicamente desarrollados y puestos en servicio con la investigación y el desarrollo científicos como única finalidad, cualquier otro sistema de IA que pueda utilizarse para llevar a cabo cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier circunstancia, toda actividad de investigación y desarrollo debe llevarse a cabo de conformidad con normas éticas y profesionales reconocidas para la investigación científica.

(12 *quater*) Habida cuenta de la naturaleza y la complejidad de la cadena de valor de los sistemas de IA, es esencial aclarar el papel de los agentes que pueden contribuir al desarrollo de los sistemas de IA, en particular de los sistemas de IA de alto riesgo. En particular, es necesario aclarar que los sistemas de IA de uso general son sistemas de IA que han sido concebidos por el proveedor para desempeñar funciones de aplicación general, como el reconocimiento de imágenes y de voz, en diversos contextos. Pueden utilizarse como sistemas de IA de alto riesgo por sí solos o ser componentes de otros sistemas de IA de alto riesgo. Por consiguiente, debido a su naturaleza particular y a fin de garantizar un reparto equitativo de las responsabilidades a lo largo de la cadena de valor de la IA, dichos sistemas deben estar sujetos a requisitos y obligaciones proporcionados y más específicos en virtud del presente Reglamento, garantizando al mismo tiempo un elevado nivel de protección de los derechos fundamentales, la salud y la seguridad. Además, los proveedores de sistemas de IA de uso general, con independencia de que estos sistemas puedan ser utilizados o no como sistemas de IA de alto riesgo por otros proveedores sin modificaciones o como componentes de sistemas de IA de alto riesgo, deben cooperar, según proceda, con los proveedores de los sistemas de IA de alto riesgo correspondientes para que puedan cumplir las obligaciones pertinentes en virtud del presente Reglamento y con las autoridades competentes establecidas en virtud del presente Reglamento. A fin de tener en cuenta las características específicas de los sistemas de IA de uso general y la rapidez de la evolución del mercado y de los avances tecnológicos en este ámbito, deben conferirse a la Comisión competencias de ejecución para especificar y adaptar la aplicación de los requisitos establecidos en el presente Reglamento a los sistemas de IA de uso general y especificar la información que deben compartir los proveedores de sistemas de IA de uso general para que los proveedores de los sistemas de IA de alto riesgo correspondientes puedan cumplir sus obligaciones en virtud del presente Reglamento.

(13) Conviene establecer normas comunes para todos los sistemas de IA de alto riesgo al objeto de garantizar un nivel elevado y coherente de protección de los intereses públicos en lo que respecta a la salud, la seguridad y los derechos fundamentales. Dichas normas deben ser coherentes con la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»), no deben ser discriminatorias y deben estar en consonancia con los compromisos de la Unión en materia de comercio internacional.

(14) Con el fin de introducir un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, es preciso aplicar un enfoque basado en los riesgos claramente definido, que adapte el tipo de las normas y su contenido a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA en cuestión. Por consiguiente, es necesario prohibir determinadas prácticas de inteligencia artificial, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, e imponer obligaciones de transparencia a determinados sistemas de IA.

(15) Al margen de los múltiples usos beneficiosos de la inteligencia artificial, dicha tecnología también puede utilizarse indebidamente y proporcionar nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social. Dichas prácticas son sumamente perjudiciales y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, libertad, igualdad, democracia y Estado de Derecho y de los derechos fundamentales que reconoce la UE, como el derecho a la no discriminación, la protección de datos y la privacidad, y los derechos del niño.

(16) Las técnicas de manipulación que posibilita la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente. La introducción en el mercado, la puesta en servicio o el uso de determinados sistemas de IA que alteran de manera sustancial el comportamiento humano, lo que hace probable que se produzcan perjuicios físicos o psicológicos, son especialmente peligrosos y, por tanto, deben prohibirse. Estos sistemas de IA utilizan componentes subliminales, como sonidos, imágenes o estímulos de vídeo, que las personas no pueden percibir, ya que dichos estímulos trascienden la percepción humana, u otras técnicas subliminales que socavan o perjudican la autonomía, la toma de decisiones o la capacidad de elegir libremente de las personas de maneras de las que las personas no son realmente conscientes, e incluso si son conscientes de ellas, no pueden controlarlas o resistirse a ellas, por ejemplo, en los ámbitos de las interfaces cerebro-máquina o la realidad virtual. Además, los sistemas de IA también pueden explotar de otro modo las vulnerabilidades de un grupo específico de personas, derivadas de su edad, su discapacidad en el sentido de la Directiva (UE) 2019/882 o de una situación social o económica específica que puede hacerlas más vulnerables a la explotación, como las personas que viven en condiciones de pobreza extrema o las minorías étnicas o religiosas. Estos sistemas de IA pueden introducirse en el mercado, ponerse en servicio o utilizarse con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona y de un modo que provoque o sea razonablemente probable que provoque perjuicios físicos o psicológicos a esa persona o a otra persona o grupo de personas, en particular perjuicios que pueden acumularse a lo largo del tiempo. La intención de distorsionar el comportamiento no puede darse por supuesta si la alteración es el resultado de factores externos al sistema de IA que escapan al control del proveedor o del usuario, es decir, factores que el proveedor o el usuario del sistema de IA no pueden prever ni mitigar razonablemente. En cualquier caso, no es necesario que el proveedor o el usuario tengan la intención de causar los perjuicios físicos o psicológicos, siempre que dichos perjuicios se deriven de las prácticas de manipulación o explotación que posibilita la IA. Las prohibiciones de tales prácticas de IA complementan las disposiciones de la Directiva 2005/29/CE, en particular la prohibición, en cualquier circunstancia, de las prácticas comerciales desleales que causan perjuicios económicos o financieros a los consumidores, hayan sido establecidas mediante de sistemas de IA o de otra manera. La prohibición de las prácticas de manipulación y explotación contenida en el presente Reglamento no debe afectar a las prácticas legales en el contexto de un tratamiento médico, por ejemplo, el tratamiento psicológico de una enfermedad mental o la rehabilitación física, cuando dichas prácticas se lleven a cabo de conformidad con las normas y la legislación médicas aplicables. Asimismo, no debe considerarse que las prácticas comerciales comunes y legítimas, conformes con la legislación aplicable son, en sí mismas, prácticas de manipulación de la IA perjudiciales.

(17) Los sistemas de IA que proporcionan una puntuación ciudadana de las personas físicas por parte de las autoridades públicas o de agentes privados pueden tener resultados discriminatorios y abocar a la exclusión a determinados grupos. Pueden menoscabar el derecho a la dignidad y la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican a las personas físicas en función de su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas o predichas. La puntuación ciudadana resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de personas físicas o grupos enteros en contextos sociales que no guardan relación con el contexto donde se generaron o recabaron los datos originalmente, 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 impliquen tales prácticas de calificación inaceptables. Esta prohibición no debe afectar a las prácticas legales de evaluación de las personas físicas realizadas para un fin específico, o para varios, de conformidad con la ley.

(18) Se considera que el uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Además, la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan «en tiempo real» acrecientan el riesgo para los derechos y las libertades de las personas afectadas por las actividades de aplicación de la ley.

(19) En consecuencia, debe prohibirse el uso de dichos sistemas con fines de aplicación de la ley, salvo en situaciones enumeradas de manera limitativa y definidas con precisión en las que su utilización es estrictamente necesaria para lograr un interés público esencial cuya importancia es superior a los riesgos. Estas situaciones son la búsqueda de posibles víctimas de un delito, incluidos menores desaparecidos; determinadas amenazas para la vida o la seguridad física de las personas físicas o amenazas de atentado terrorista; y la detección, la localización, la identificación o el enjuiciamiento de los autores o sospechosos de los delitos mencionados en la Decisión Marco 2002/584/JAI del Consejo[9], si la normativa del Estado miembro implicado señala una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos de tres años, tal como se definan en el Derecho de dicho Estado miembro. Fijar ese umbral para la pena o la medida de seguridad privativas de libertad con arreglo al Derecho nacional contribuye a garantizar que el delito sea lo suficientemente grave como para llegar a justificar el uso de sistemas de identificación biométrica remota «en tiempo real». Por otro lado, en la práctica, algunos de los treinta y dos delitos enumerados en la Decisión Marco 2002/584/JAI del Consejo son probablemente más relevantes que otros en el sentido de que, previsiblemente, recurrir a la identificación biométrica remota «en tiempo real» se considerará necesario y proporcionado en grados muy distintos para llevar a cabo la detección, la localización, la identificación o el enjuiciamiento de los autores o sospechosos de tales delitos, como también habrá enormes diferencias en la gravedad, la probabilidad y la magnitud de los perjuicios o las posibles consecuencias negativas que se deriven de ellos. Además, el presente Reglamento debe preservar la capacidad de las autoridades encargadas de la aplicación de la ley, del control fronterizo, de la inmigración o del asilo para llevar a cabo controles de identidad en presencia de la persona afectada, de conformidad con las condiciones establecidas en el Derecho de la Unión y en el Derecho nacional para estos controles. En particular, las autoridades encargadas de la aplicación de la ley, del control fronterizo, de la inmigración o del asilo deben poder utilizar sistemas de información, de conformidad con el Derecho de la Unión o el Derecho nacional, para identificar a una persona que, durante un control de identidad, se niegue a ser identificada o no pueda declarar o demostrar su identidad, sin que el presente Reglamento exija que se obtenga 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 una afección médica, revelar su identidad a las autoridades encargadas de la aplicación de la ley.

[9] 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) Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas situaciones enumeradas de manera limitativa y definidas con precisión, deben tenerse en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las salvaguardias y condiciones que acompañen a su uso. Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar sujeto a límites temporales y espaciales adecuados que tengan en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. La base de datos de personas de referencia debe ser adecuada para cada caso de uso en cada una de las situaciones antes mencionadas.

(21) Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro. En principio, dicha autorización debe obtenerse antes de que se utilice el sistema con el fin de identificar a una o varias personas. Deben permitirse excepciones a esta norma en situaciones de urgencia debidamente justificadas, es decir, aquellas en las que la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso. En tales situaciones de urgencia, el uso debe limitarse al mínimo imprescindible y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno y según corresponda en cada caso concreto de uso urgente por parte de las autoridades encargadas de la aplicación de la ley. Además, en esas situaciones las autoridades encargadas de la aplicación de la ley deben tratar de obtener una autorización lo antes posible e indicar los motivos por los que no han podido hacerlo antes.

(22) Por otro lado, conviene estipular, en el marco exhaustivo que establece este Reglamento, que dicho uso en el territorio de un Estado miembro conforme a lo dispuesto en el presente Reglamento solo debe ser posible cuando el Estado miembro en cuestión haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho interno, y en la medida en que lo haya contemplado. En consecuencia, con el presente Reglamento los Estados miembros siguen siendo libres de no ofrecer esta posibilidad en absoluto o de ofrecerla únicamente en relación con algunos de los objetivos que pueden justificar un uso autorizado conforme al presente Reglamento.

(23) La utilización de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley implica, necesariamente, el tratamiento de datos biométricos. Las normas del presente Reglamento que prohíben, con algunas excepciones, ese uso, basadas en el artículo 16 del TFUE, deben aplicarse como *lex specialis* con respecto a las normas sobre el tratamiento de datos biométricos que figuran en el artículo 10 de la Directiva (UE) 2016/680, con lo que se regula de manera exhaustiva dicho uso y el tratamiento de los datos biométricos conexos. Por lo tanto, ese 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 un margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines de aplicación de la ley, utilicen tales sistemas y traten los datos conexos en los supuestos previstos en el artículo 10 de la Directiva (UE) 2016/680. En este contexto, el presente Reglamento no pretende sentar la base jurídica para el tratamiento de datos personales en virtud del artículo 8 de la Directiva (UE) 2016/680. Sin embargo, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines distintos de la aplicación de la ley, incluso por parte de las autoridades competentes, no debe estar cubierto por el marco específico establecido por el presente Reglamento en lo que respecta al uso de dichos sistemas con fines de aplicación de la ley. Por consiguiente, su uso con fines distintos de la aplicación de la ley no debe supeditarse al requisito de obtener una autorización previsto en este Reglamento ni a las normas detalladas del Derecho interno aplicables que pudieran hacerlo efectivo.

(24) Todo tratamiento de datos biométricos y de datos personales de otra índole asociado al uso de sistemas de IA con fines de identificación biométrica no asociado al uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley regulado por el presente Reglamento debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. 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 con el fin de identificar de manera unívoca a una persona física con fines distintos de la aplicación de la ley, a menos que se dé una de las circunstancias contempladas en el párrafo segundo de estos dos artículos.

(25) 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 queda obligada por las normas establecidas en el artículo 5, apartado 1, letra d), y el artículo 5, apartados 2, 3 y 4, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE, que se refieren al tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE, en la medida en que no Irlanda no quede obligada por las normas que regulen formas de cooperación judicial en materia penal o de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas sobre la base del artículo 16 del TFUE.

(26) De conformidad con lo dispuesto en los artículos 2 y 2 *bis* del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no queda obligada las normas establecidas en el artículo 5, apartado 1, letra d), y el artículo 5, apartados 2, 3 y 4, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE, que se relacionen con el tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE, ni está sujeta a su aplicación.

(27) La introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo en la Unión debe supeditarse al cumplimiento por su parte de determinados requisitos obligatorios, los cuales deben garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuya información de salida se utilice en la Unión no entrañen riesgos inaceptables para intereses públicos importantes de la UE, reconocidos y protegidos por el Derecho de la Unión. La calificación «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional, si la hubiera.

(28) Los sistemas de IA pueden tener efectos adversos para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de productos. 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 velar por que solo lleguen al mercado aquellos productos que sean seguros y conformes, es importante prevenir y reducir debidamente los riesgos de seguridad que pueda generar un producto en su conjunto debido a sus componentes digitales, entre los que pueden figurar los sistemas de IA. Por ejemplo, los robots cada vez más autónomos que se utilizan en las fábricas o con fines de asistencia y cuidado personal deben poder funcionar y desempeñar sus funciones de manera segura en entornos complejos. Del mismo modo, en el sector sanitario, donde los riesgos para la vida y la salud son especialmente elevados, los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, deben ser fiables y precisos. La magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es particularmente pertinente cuando este es clasificado como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además de esos derechos, conviene poner de relieve que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta de la UE y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan en mayor profundidad en la observación general n.º 25 del Comité de los Derechos del Niño relativa a los derechos de los niños en relación con el entorno digital. Ambos instrumentos exigen que se tengan en consideración las vulnerabilidades de los menores y que se les brinde la protección y la asistencia necesarias para su bienestar. Cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, en particular en lo que respecta a la salud y la seguridad de las personas, también se debe tener en cuenta el derecho fundamental a un nivel elevado de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión.

(29) En cuanto 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 que entran en el ámbito de aplicación del Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo[10], el Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo[11], el Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo[12], la Directiva 2014/90/UE del Parlamento Europeo y del Consejo[13], la Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo[14], el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo[15], el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo[16], y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo[17], procede modificar dichos actos para garantizar que, cuando la Comisión adopte en el futuro adopte actos delegados o de ejecución pertinentes en la materia basándose en ellos, tenga en cuenta los requisitos obligatorios para los sistemas de IA de alto riesgo previstos en el presente Reglamento, atendiendo a las particularidades técnicas y reglamentarias de los distintos sectores y sin interferir con la gobernanza, los mecanismos de evaluación de la conformidad y supervisión, y las autoridades existentes en cada uno de ellos.

---

10 Reglamento (CE) n.º 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) n.º 2320/2002 (DO L 97 de 9.4.2008, p. 72).

11 Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 1).

12 Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 52).

13 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).

14 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).

15 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 sus remolques y de los sistemas, los componentes y las 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 por el que se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1).

16 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 la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010, (CE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y 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).

17 Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los 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 de la Comisión (DO L 325 de 16.12.2019, p 1).

(30) En cuanto a los sistemas de IA que son componentes de seguridad de productos, o que son productos en sí mismos, y entran dentro del ámbito de aplicación de determinada legislación de armonización de la Unión, procede considerarlos de alto riesgo en virtud del presente Reglamento si el producto en cuestión es sometido al procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad externo de acuerdo con dicha legislación de armonización pertinente de la Unión. Esos productos son, en concreto, máquinas, juguetes, ascensores, equipo y sistemas de protección para uso en atmósferas potencialmente explosivas, equipos radioeléctricos, equipos a presión, equipo de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios y productos sanitarios para diagnóstico *in vitro*.

(31) Que un sistema de IA se considere de alto riesgo en virtud del presente Reglamento no significa necesariamente que el producto del que sea componente de seguridad, o el sistema de IA en sí mismo como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto. Tal es el caso, en particular, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo[18] y del Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo[19], que prevén que un organismo independiente realice una evaluación de la conformidad de los productos de riesgo medio y alto.

[18] Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los 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 por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

[19] Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los 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).

(32) En cuanto a los sistemas de IA de alto riesgo que no son componentes de seguridad de productos o no son productos en sí mismos, hay que considerarlos de alto riesgo si, a la luz de su finalidad prevista, presentan un alto riesgo de menoscabar la salud y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca, y se utilizan en varias esferas predefinidas especificadas en el presente Reglamento. Para identificar dichos sistemas se emplean la misma metodología y los mismos criterios previstos para la posible modificación futura de la lista de sistemas de IA de alto riesgo. También es importante aclarar que, en los supuestos de alto riesgo mencionados en el anexo III, puede haber sistemas que no entrañen un riesgo considerable para los intereses jurídicos protegidos en esos supuestos, teniendo en cuenta la información de salida producida por el sistema de IA. Por lo tanto, solo cuando dicha información de salida tenga un alto grado de importancia (es decir, no sea meramente accesoria) respecto de la acción o decisión pertinente, de tal manera que suponga un riesgo considerable para los intereses jurídicos que se protegen, el sistema de IA que genera dicha información de salida debe considerarse de alto riesgo. Por ejemplo, cuando la información facilitada por un sistema de IA al ser humano consista en la elaboración de perfiles de personas físicas en el sentido del artículo 4, apartado 4, del Reglamento (UE) 2016/679, del artículo 3, apartado 4, de la Directiva (UE) 2016/680 y del artículo 3, apartado 5, del Reglamento (UE) 2018/1725, dicha información no debe considerarse normalmente de carácter accesorio en el contexto de los sistemas de IA de alto riesgo a que se refiere el anexo III. No obstante, si la información de salida del sistema de IA tiene una importancia insignificante o menor para la acción o la decisión humanas, el sistema puede considerarse meramente accesorio. Es el caso, por ejemplo, de los sistemas de IA utilizados para la traducción con fines informativos o para la gestión de documentos.

(33) Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener consecuencias discriminatorias. Esto es especialmente importante en lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Por este motivo, debe considerarse que los sistemas de identificación biométrica remota «en tiempo real» y «en diferido» conllevan un alto riesgo. Debido a los riesgos que entrañan, deben aplicarse requisitos específicos referentes a las capacidades de registro y la vigilancia humana a ambos tipos de sistemas de identificación biométrica remota.

(34) En el caso de la gestión y el funcionamiento de infraestructuras críticas, conviene considerar de alto riesgo a los sistemas de IA destinados a ser componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas que se enumeran en el anexo I, punto 8, de la Directiva relativa a la resiliencia de las entidades críticas, el tráfico rodado y el suministro de agua, gas, calefacción y electricidad, pues su fallo o defecto de funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y alterar de manera apreciable el desarrollo habitual de las actividades sociales y económicas. Los componentes de seguridad de las infraestructuras críticas, por ejemplo, de 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 el funcionamiento del sistema. Un fallo o un defecto de funcionamiento de estos componentes podría dar lugar directamente a riesgos para la integridad física de las infraestructuras críticas y, por tanto, a riesgos para la salud y la seguridad de las personas y los bienes. Los componentes destinados a ser utilizados exclusivamente con fines de ciberseguridad no deben considerarse componentes de seguridad. Entre los componentes de seguridad de esas infraestructuras críticas cabe citar los sistemas de control de la presión del agua o los sistemas de control de las alarmas contra incendios en los centros de computación en la nube.

(35) Deben considerarse de alto riesgo los sistemas de IA que se utilizan en la educación o la formación profesional, y en especial aquellos que determinan el acceso o la admisión a programas o centros educativos y de formación profesional a todos los niveles, o que distribuyen a las personas entre dichos centros o programas, o aquellos que evalúan los resultados del aprendizaje de las personas, ya que pueden determinar la trayectoria formativa y profesional de una persona y, en consecuencia, afectar a su capacidad para asegurar su subsistencia. Cuando no se diseñan y utilizan correctamente, estos sistemas pueden violar el derecho a la educación y la formación, y el derecho a no sufrir discriminación, además de perpetuar patrones históricos de discriminación.

(36) También deben considerarse de alto riesgo los sistemas de IA que se utilizan en el empleo, la gestión de los trabajadores y el acceso al autoempleo, sobre todo para la contratación y la selección de personal; para la toma de decisiones relativas a la promoción y la rescisión de contratos; y para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales y el seguimiento o la evaluación de personas en relaciones contractuales de índole laboral, dado que pueden afectar de un modo considerable a las futuras perspectivas laborales y los medios de subsistencia de dichas personas. Las relaciones contractuales de índole laboral deben implicar a los empleados y las personas que prestan servicios a través de plataformas, como indica el Programa de trabajo de la Comisión para 2021. En principio, esas personas no deben ser consideradas usuarios en el sentido del presente Reglamento. Dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, ciertos grupos de edad, personas con discapacidad o personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, la promoción o la retención de personas en relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden afectar a sus derechos a la protección de los datos personales y a la privacidad.

(37) El acceso y el disfrute de determinados servicios y ayudas esenciales de carácter público y privado necesarios para que las personas participen en la sociedad o cuenten con unas condiciones de vida mejores es otro ámbito en el que conviene prestar especial atención a la utilización de sistemas de IA. En concreto, deben considerarse de alto riesgo los sistemas de IA usados para evaluar la calificación crediticia o solvencia de personas físicas, ya que deciden si dichas personas pueden acceder a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA usados con este fin pueden discriminar a personas o grupos y perpetuar patrones históricos de discriminación, por ejemplo, por motivos de origen racial o étnico, discapacidad, edad u orientación sexual, o generar nuevas formas de efectos discriminatorios. Habida cuenta del alcance sumamente limitado de su impacto y de las escasas alternativas disponibles en el mercado, conviene dejar exentos a los sistemas de IA destinados a evaluar la solvencia y a la calificación crediticia cuando los pongan en servicio, para su propio uso, microempresas o pequeñas empresas, tal como se definen en el anexo de la Recomendación 2003/361/CE de la Comisión. Las personas físicas que solicitan o reciben ayudas y servicios esenciales de autoridades públicas suelen depender de ellos y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. Si se utilizan sistemas de IA para decidir si las autoridades deben denegar, reducir, revocar o reclamar dichas ayudas y servicios, y para decidir si los beneficiarios tienen legítimamente derecho a dichas ayudas o servicios, estos sistemas pueden afectar de un modo considerable a los medios de subsistencia de las personas y podrían infringir sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a una tutela judicial efectiva. Por lo tanto, esos sistemas deben considerarse de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y el uso de enfoques innovadores en la Administración pública, que se beneficiarían de una mayor utilización de sistemas de IA conformes y seguros, siempre y cuando dichos sistemas no conlleven un alto riesgo para las personas jurídicas y físicas. Por último, los sistemas de IA empleados para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia también deben considerarse de alto riesgo, dado que adoptan decisiones en situaciones sumamente críticas para la vida y la salud de las personas y de sus bienes. Los sistemas de IA también se utilizan cada vez más para la evaluación de riesgos en relación con las personas físicas y la fijación de precios en el caso de los seguros de vida y de salud y, si no se diseñan, desarrollan y utilizan debidamente, pueden tener graves consecuencias para la vida y la salud de las personas, como la exclusión financiera y la discriminación. Para garantizar un enfoque coherente en el sector de los servicios financieros, debe aplicarse la excepción antes mencionada en relación con las microempresas o pequeñas empresas y su propio uso, en la medida en que ellas mismas proporcionen y pongan en servicio un sistema de IA con el fin de vender sus propios productos de seguros.

(38) Las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta. En particular, si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos oportunos en términos de precisión o solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, puede señalar a personas de manera discriminatoria, incorrecta o injusta. Además, podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como los derechos de la defensa y la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén bien documentados. Por consiguiente, procede considerar de alto riesgo a múltiples sistemas de IA diseñados para usarse con fines de aplicación de la ley cuando su precisión, fiabilidad y transparencia sean especialmente importantes para evitar consecuencias adversas, conservar la confianza de la población y garantizar la rendición de cuentas y una compensación efectiva. En vista de la naturaleza de las actividades en cuestión y de los riesgos conexos, entre dichos sistemas de IA de alto riesgo deben incluirse, en particular, los sistemas de IA que las autoridades encargadas de la aplicación de la ley utilicen para realizar evaluaciones del riesgo individuales, los polígrafos y herramientas similares, o los sistemas utilizados para detectar el estado emocional de una persona física; para evaluar la fiabilidad de las pruebas en un proceso penal; para predecir la comisión o reiteración de un delito real o potencial mediante la elaboración de perfiles de personas físicas; para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o grupos; para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de infracciones penales. No debe considerarse que los sistemas de IA destinados específicamente a que los utilicen en procesos administrativos las autoridades fiscales y aduaneras y las unidades de inteligencia financiera que llevan a cabo tareas administrativas de análisis de información de conformidad con la legislación de la Unión para luchar contra el blanqueo de capitales son sistemas de IA de alto riesgo usados por las autoridades encargadas de la aplicación de la ley con el fin de prevenir, detectar, investigar y enjuiciar infracciones penales.

(39) Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilizan en estos contextos sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, sus derechos a la libre circulación, la no discriminación, la intimidad personal y la protección de los datos personales, la protección internacional y la buena administración. Por lo tanto, procede considerar de alto riesgo a aquellos sistemas de IA destinados a que las autoridades públicas competentes que realizan tareas en el ámbito de la gestión de la migración, el asilo y el control fronterizo los utilicen como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; para evaluar determinados riesgos que presenten personas físicas que entren en el territorio de un Estado miembro o soliciten un visado o asilo; para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes de un estatuto reúnen los requisitos necesarios para su obtención. Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo abarcados por el presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por la Directiva 2013/32/UE del Parlamento Europeo y del Consejo[20], el Reglamento (UE) n.º 810/2009 del Parlamento Europeo y el Consejo[21], y otra legislación en la materia.

[20] Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional (DO L 180 de 29.6.2013, p. 60).

[21] Reglamento (CE) n.º 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).

(40) Deben considerarse de alto riesgo ciertos sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede considerar de alto riesgo aquellos sistemas de IA cuyo objetivo es ayudar a las autoridades judiciales a interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. No obstante, dicha clasificación no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia en casos concretos, como la anonimización o seudonimización de las resoluciones judiciales, documentos o datos; la comunicación entre los miembros del personal; tareas administrativas.

(41) El hecho de que un sistema de IA sea considerado de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea legal con arreglo a otros actos del Derecho de la Unión o del Derecho interno compatible con el Derecho de la Unión relativo a la protección de los datos personales o a la utilización de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Todo uso de ese tipo debe seguir realizándose exclusivamente en consonancia con los requisitos oportunos derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho interno. No debe entenderse que el presente Reglamento constituye el fundamento jurídico para el tratamiento de datos personales, incluidas categorías especiales de datos personales, cuando sea pertinente, salvo que el presente Reglamento disponga específicamente otra cosa.

(42) Con el objetivo de mitigar los riesgos que presentan los sistemas de IA de alto riesgo que se introducen en el mercado o ponen en servicio en la Unión, es preciso aplicar ciertos requisitos obligatorios que tengan en cuenta la finalidad prevista del uso del sistema y estén en consonancia con el sistema de gestión de riesgos que debe establecer el proveedor. En particular, el sistema de gestión de riesgos debe consistir en un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo. Este proceso debe garantizar que el proveedor identifique y analice los riesgos para la salud, la seguridad y los derechos fundamentales de las personas que puedan verse afectadas por el sistema habida cuenta de su finalidad prevista, incluidos los posibles riesgos derivados de la interacción entre el sistema de IA y el entorno en el que opera, y, en consecuencia, adopte medidas adecuadas de gestión de riesgos a la vista del estado de la técnica.

(43) Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la calidad de los conjuntos de datos utilizados, la documentación técnica y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales, según corresponda en función de la finalidad prevista del sistema, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, con lo que se evitan restricciones injustificadas de este.

(44) Muchos sistemas de IA necesitan datos de alta calidad para funcionar correctamente, en especial cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione del modo previsto y en condiciones de seguridad y no se convierta en la fuente de alguno de los tipos de discriminación prohibidos por el Derecho de la Unión. Es preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos de entrenamiento, validación y prueba sean de buena calidad. Los conjuntos de datos de entrenamiento, validación y prueba deben ser lo suficientemente pertinentes y representativos y tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en las que en un principio se usará el sistema de IA de alto riesgo. Estos conjuntos de datos también deben estar lo más libres de errores y ser lo más completos posible en vista de la finalidad prevista del sistema de IA, teniendo en cuenta, de manera proporcionada, la viabilidad técnica y los últimos avances, la disponibilidad de los datos y la aplicación de medidas adecuadas de gestión de riesgos, de modo que se afronten debidamente las posibles deficiencias de los conjuntos de datos. El requisito de que los conjuntos de datos sean completos y carezcan de errores no debe afectar al uso de técnicas de protección de la privacidad en el contexto del desarrollo y la prueba de sistemas de IA. Los conjuntos de datos de entrenamiento, validación y prueba deben tener en cuenta, en la medida necesaria para su finalidad prevista, los rasgos, características o elementos particulares del entorno o contexto geográfico, funcional o de comportamiento específico en el que se pretende utilizar el sistema de IA. Con el fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725, para garantizar que el sesgo de los sistemas de IA de alto riesgo se vigile, detecte y corrija.

(44 *bis*) Al aplicar los principios a que se refieren el artículo 5, apartado 1, letra c), del Reglamento (UE) 2016/679 y el artículo 4, apartado 1, letra c), del Reglamento (UE) 2018/1725, en particular el principio de minimización de datos, en lo que respecta a los conjuntos de datos de entrenamiento, validación y prueba previstos en el presente Reglamento, debe tenerse debidamente en cuenta el ciclo de vida completo del sistema de IA.

(45) Para poder desarrollar sistemas de IA de alto riesgo, determinados agentes, tales como proveedores, organismos notificados y otras entidades pertinentes, como centros de innovación digital, centros de ensayo y experimentación e investigadores, deben tener acceso a conjuntos de datos de alta calidad en sus respectivos campos de actividad relacionados con el presente Reglamento y poder utilizarlos. Los espacios comunes europeos de datos establecidos por la Comisión y la facilitación del intercambio de datos entre empresas y con los Gobiernos en aras del interés público serán esenciales para brindar un acceso fiable, responsable y no discriminatorio a datos de alta calidad con los que entrenar, validar y probar los sistemas de IA. Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a datos sanitarios y el entrenamiento, a partir de esos conjuntos de datos, de algoritmos de inteligencia artificial de una manera segura, oportuna, transparente y fiable que respete la privacidad, y contando con la debida gobernanza institucional. Las autoridades competentes pertinentes, incluidas las sectoriales, que proporcionan acceso a datos o lo facilitan también pueden contribuir al suministro de datos de alta calidad orientados a entrenar, validar y probar sistemas de IA.

(46) Para verificar si los sistemas de IA de alto riesgo cumplen los requisitos previstos en el presente Reglamento, resulta esencial disponer de información sobre el modo en que se han desarrollado y sobre su funcionamiento durante todo su ciclo de vida. A tal fin, es preciso llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA en cuestión cumple los requisitos pertinentes. Dicha información debe incluir, en particular, las características, capacidades y limitaciones generales del sistema; los algoritmos; los datos; los procesos de entrenamiento, prueba y validación empleados, y documentación sobre el sistema de gestión de riesgos pertinente. La documentación técnica debe mantenerse actualizada. Además, los proveedores o usuarios deben conservar los archivos de registro generados automáticamente por el sistema de IA de alto riesgo, incluidos, por ejemplo, los datos de salida, la fecha y hora de inicio, etc., en la medida en que dicho sistema y los archivos de registro correspondientes estén bajo su control, durante un período adecuado para permitirles cumplir sus obligaciones.

(47) Por otro lado, debe exigirse cierto grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas. Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e incluir información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y riesgos de discriminación de las personas que puedan verse afectadas por el sistema en vista de su finalidad prevista, cuando corresponda. Para facilitar que los usuarios comprendan las instrucciones de uso, estas deben contener ejemplos ilustrativos, según proceda.

(48) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que su funcionamiento pueda ser vigilado por personas físicas. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de vigilancia humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema esté sujeto a limitaciones operativas incorporadas que el propio sistema no pueda desactivar, que responda al operador humano, y que las personas físicas a quienes se haya encomendado la vigilancia humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función. Teniendo en cuenta las enormes consecuencias que tienen para las personas las correspondencias incorrectas de determinados sistemas de identificación biométrica, conviene establecer un requisito de supervisión humana reforzada para dichos sistemas, de modo que el usuario no pueda tomar ninguna medida ni decisión sobre la base de la identificación resultante del sistema, salvo si al menos dos personas físicas lo han verificado y confirmado por separado. Dichas personas podrían proceder de una o varias entidades e incluir a la persona que explota o utiliza el sistema. Este requisito no debe suponer una carga ni retrasos innecesarios y podría bastar con que las verificaciones separadas por parte de las distintas personas se registren automáticamente en los registros generados por el sistema.

(49) Los sistemas de IA de alto riesgo deben funcionar de manera consistente durante todo su ciclo de vida y presentar un nivel adecuado de precisión, solidez y ciberseguridad con arreglo al estado de la técnica generalmente reconocido. En este sentido, debe comunicarse a los usuarios el nivel de precisión y los parámetros empleados para medirla.

(50) La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo, que deben ser resilientes en relación con los comportamientos perjudiciales o de otro modo indeseables que puedan derivarse de limitaciones en los sistemas o en el entorno en el que estos funcionan (p. ej., errores, fallos, incoherencias o situaciones inesperadas). Por consiguiente, los sistemas de IA de alto riesgo deben diseñarse y desarrollarse con soluciones técnicas adecuadas para prevenir o minimizar ese comportamiento perjudicial o indeseable, como, por ejemplo, mecanismos que permitan al sistema interrumpir de forma segura su funcionamiento (planes de prevención contra fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de determinados límites predeterminados. La incapacidad de protegerlos frente a estos riesgos podría tener consecuencias para la seguridad o afectar de manera negativa a los derechos fundamentales, por ejemplo, debido a la adopción de decisiones equivocadas o a que el sistema de IA en cuestión genere una información de salida errónea o sesgada.

(51) La ciberseguridad es fundamental para garantizar que los sistemas de IA resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema, traten de alterar su uso, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad. Los ciberataques contra sistemas de IA pueden dirigirse contra elementos específicos de la IA, como los conjuntos de datos de entrenamiento (p. ej., contaminación de datos) o los modelos entrenados (p. ej., ataques adversarios), o aprovechar las vulnerabilidades de los elementos digitales del sistema de IA o la infraestructura de TIC subyacente. Por lo tanto, para asegurar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente.

(52) Como parte de la legislación de armonización de la Unión, conviene que las normas aplicables a la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA de alto riesgo se establezcan en consonancia con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo[22] por el que se establecen los requisitos de acreditación y vigilancia del mercado de los productos, la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo[23] sobre un marco común para la comercialización de los productos y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo[24] relativo a la vigilancia del mercado y la conformidad de los productos (en lo sucesivo, el «nuevo marco legislativo para la comercialización de productos»).

(52 *bis*) En consonancia con los principios del nuevo marco legislativo, deben establecerse obligaciones específicas para los operadores pertinentes dentro de la cadena de valor de la IA para garantizar la seguridad jurídica y facilitar el cumplimiento del presente Reglamento. En determinadas situaciones, esos operadores podrían desempeñar más de una función al mismo tiempo y, por lo tanto, deben cumplir de forma conjunta todas las obligaciones pertinentes asociadas a dichas funciones. Por ejemplo, un operador podría actuar como distribuidor e importador al mismo tiempo.

(53) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad asociada a la introducción en el mercado o puesta en servicio de un sistema de IA de alto riesgo, con independencia de si dicha persona física o jurídica es o no quien diseñó o desarrolló el sistema.

---

22 Reglamento (CE) n.º 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) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

23 Decisión n.º 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).

24 Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la 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).

(54) El proveedor debe instaurar un sistema de gestión de la calidad sólido, velar por que se siga el procedimiento de evaluación de la conformidad necesario, elaborar la documentación pertinente y establecer un sistema sólido de vigilancia poscomercialización. Las autoridades públicas que pongan en servicio sistemas de IA de alto riesgo para su propio uso pueden aprobar y aplicar las normas que regulen el sistema de gestión de la calidad en el marco del sistema de gestión de la calidad adoptado a escala nacional o regional, según proceda, teniendo en cuenta las particularidades del sector y las competencias y la organización de la autoridad pública en cuestión.

(54 *bis*) Para garantizar la seguridad jurídica, es necesario aclarar que, en determinadas condiciones específicas, cualquier persona física o jurídica debe ser considerada proveedor de un nuevo sistema de IA de alto riesgo y, por tanto, asumir todas las obligaciones pertinentes. Sería así, por ejemplo, si esa persona pone su nombre o marca comercial en un sistema de IA de alto riesgo ya introducido en el mercado o puesto en servicio, o si modifica la finalidad prevista de un sistema de IA que no sea de alto riesgo y que ya se haya introducido en el mercado o puesto en servicio de manera que el sistema modificado se convierta en un sistema de IA de alto riesgo. Estas disposiciones deben aplicarse sin perjuicio de las disposiciones más específicas establecidas en la legislación sectorial del nuevo marco legislativo junto con la que 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 al cumplimiento de los requisitos aplicables, debe seguir aplicándose a los sistemas de IA de alto riesgo que sean productos sanitarios en el sentido de dicho Reglamento.

(55) Cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto recogido en un acto legislativo sectorial pertinente del nuevo marco legislativo no se introduzca en el mercado ni se ponga en servicio independientemente del producto, el fabricante del producto, tal como se define en el acto legislativo pertinente del nuevo marco legislativo, debe cumplir las obligaciones que el presente Reglamento impone al proveedor y asegurarse especialmente de que el sistema de IA integrado en el producto final cumpla con los requisitos del presente Reglamento.

(56) Para facilitar la aplicación del presente Reglamento y ofrecer igualdad de condiciones a los operadores, es importante velar por que una persona establecida en la Unión pueda, en cualquier circunstancia, facilitar a las autoridades toda la información necesaria sobre el cumplimiento de un sistema de IA, teniendo en cuenta las distintas formas en que se pueden proporcionar productos digitales. Por lo tanto, cuando no se pueda identificar a un importador, antes de ofrecer sus sistemas de IA en la Unión los proveedores establecidos fuera de su territorio tendrán que designar, mediante un mandato escrito, a un representante autorizado que se encuentre en la Unión.

(56 *bis*) Para los proveedores que no estén establecidos en la Unión, el representante autorizado desempeña un papel fundamental a la hora de garantizar la conformidad de los sistemas de IA de alto riesgo introducidos en el mercado o puestos en servicio en la Unión por esos proveedores y de servir de persona de contacto establecida en la Unión. Dado este papel fundamental, y con el fin de garantizar que se asuma la responsabilidad a efectos de la aplicación del presente Reglamento, es conveniente que el representante autorizado sea responsable solidario junto con el proveedor de los sistemas de IA de alto riesgo defectuosos. La responsabilidad del representante autorizado prevista en el presente Reglamento se entenderá sin perjuicio de las disposiciones de la Directiva 85/374/CEE sobre la responsabilidad por los daños causados por productos defectuosos.

(57) [suprimido]

(58) Habida cuenta de las características de los sistemas de IA y de los riesgos que su uso puede conllevar para la seguridad y los derechos fundamentales, también en lo que respecta a la necesidad de garantizar la correcta vigilancia del funcionamiento de un sistema de IA en un contexto real, conviene definir las responsabilidades específicas de los usuarios. En particular, los usuarios deben utilizar los sistemas de IA de alto riesgo conforme a las instrucciones de uso. Además, es preciso definir otras obligaciones en relación con la vigilancia del funcionamiento de los sistemas de IA y con el registro, según proceda. Estas obligaciones no deben afectar a otras obligaciones de los usuarios en relación con los sistemas de IA de alto riesgo en virtud del Derecho nacional o de la Unión, y no deben aplicarse cuando su uso se enmarque en una actividad personal de carácter no profesional.

(58 *bis*) Conviene aclarar que el presente Reglamento no afecta a las obligaciones de los proveedores y usuarios de sistemas de IA en su papel de responsables o encargados del tratamiento derivado del Derecho de la Unión 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 confiere dicho Derecho de la Unión, incluidos los derechos relacionados con la toma de decisiones individuales de forma totalmente automatizada, como la elaboración de perfiles. Unas normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA establecidas en virtud del presente Reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el Derecho de la Unión en materia de protección de datos personales y otros derechos fundamentales.

(59) [suprimido]

(60) [suprimido]

(61) La normalización debe desempeñar un papel fundamental para proporcionar soluciones técnicas a los proveedores a fin de garantizar el cumplimiento del presente Reglamento, en consonancia con los últimos avances. El cumplimiento de las normas armonizadas definidas en el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[25], que generalmente se espera que reflejen los últimos avances, debe ser un medio para que los proveedores demuestren su conformidad con los requisitos previstos en el presente Reglamento. No obstante, a falta de referencias pertinentes a las normas armonizadas, la Comisión debe poder establecer, mediante actos de ejecución, especificaciones comunes para determinados requisitos previstos en el presente Reglamento como solución alternativa excepcional para facilitar la obligación del proveedor de cumplir los requisitos del presente Reglamento, cuando el proceso de normalización esté bloqueado o cuando haya retrasos en el establecimiento de una norma armonizada adecuada. Si dichos retrasos se deben a la complejidad técnica de la norma en cuestión, la Comisión debe tenerlo en cuenta antes de considerar la posibilidad de establecer especificaciones comunes. Una participación adecuada de las pequeñas y medianas empresas en la elaboración de normas que apoyen la aplicación del presente Reglamento es esencial para promover la innovación y la competitividad en el ámbito de la inteligencia artificial dentro de la Unión. Dicha participación debe garantizarse adecuadamente de conformidad con los artículos 5 y 6 del Reglamento (UE) n.º 1025/2012.

[25] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, 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 por el que se deroga 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).

(61 *bis*) Conviene que, sin perjuicio del uso de normas armonizadas y especificaciones comunes, los proveedores se beneficien de una presunción de conformidad con el requisito pertinente en materia de datos cuando su sistema de IA de alto riesgo haya sido entrenado y probado con datos que reflejen el entorno geográfico, funcional o de comportamiento específico en el que se pretende utilizar el sistema de IA. Del mismo modo, de conformidad con el artículo 54, apartado 3, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, debe presumirse que los sistemas de IA de alto riesgo que cuenten con una certificación o declaración de conformidad en virtud de un esquema 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. Esto se entiende sin perjuicio del carácter voluntario de dicho esquema de ciberseguridad.

(62) Antes de su introducción en el mercado o puesta en servicio, los sistemas de IA de alto riesgo deben someterse a una evaluación de la conformidad que garantice que son altamente fiables.

(63) En el caso de los sistemas de IA de alto riesgo asociados a productos cubiertos por la legislación de armonización vigente en la Unión que sigue el planteamiento del nuevo marco legislativo, conviene que la evaluación de si cumplen o no los requisitos establecidos en el presente Reglamento se enmarque en la evaluación de la conformidad ya prevista en dicha legislación. De este modo, se reducirá al mínimo la carga que deben soportar los operadores y se evitarán posibles duplicidades. Por lo tanto, 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 prevista en la legislación pertinente del nuevo marco legislativo. Este planteamiento se refleja totalmente en la interrelación entre el presente Reglamento y el [Reglamento relativo a las máquinas]. Si bien los requisitos definidos en el presente Reglamento abordan los riesgos de seguridad de los sistemas de IA que desempeñan funciones de seguridad en máquinas, algunos de los requisitos específicos establecidos en el [Reglamento relativo a las máquinas] garantizarán la integración segura del sistema de IA en la máquina general, con el fin de no poner en peligro la seguridad de la máquina en su conjunto. El [Reglamento relativo a las máquinas] aplica la misma definición de «sistema de IA» que el presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo relacionados con productos regulados por los Reglamentos 745/2017 y 746/2017 sobre los productos sanitarios, la aplicabilidad de los requisitos del presente Reglamento debe entenderse sin perjuicio de la lógica de gestión de riesgos ni de la evaluación de la relación beneficio-riesgo realizada en el marco de los productos sanitarios y tener en cuenta ambos elementos.

(64) Puesto que los profesionales que realizan la certificación previa a la comercialización tienen una experiencia más amplia en el campo de la seguridad de los productos, y habida cuenta de la diferente naturaleza de los riesgos implicados, procede limitar, al menos en la fase inicial de aplicación del presente Reglamento, el alcance de las evaluaciones de la conformidad realizadas por terceros a los sistemas de IA de alto riesgo que no están asociados a productos. En consecuencia, el proveedor es quien, por norma general, debe llevar a cabo la evaluación de la conformidad de dichos sistemas bajo su propia responsabilidad, con la única excepción de los sistemas de IA que están destinados a utilizarse para la identificación biométrica remota de personas. En el caso de estos últimos, y en la medida en que no estén prohibidos, debe preverse que un organismo notificado participe en la evaluación de la conformidad.

(65) En virtud del presente Reglamento, las autoridades nacionales competentes deben notificar a los organismos notificados que realizarán la evaluación externa de la conformidad de los sistemas de IA destinados a utilizarse para la identificación biométrica remota de personas, siempre y cuando cumplan una serie de requisitos, fundamentalmente en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses. La notificación de dichos organismos debe ser enviada por las autoridades nacionales competentes a la Comisión y a los demás Estados miembros a través de la herramienta de notificación electrónica desarrollada y gestionada por la Comisión de conformidad con el artículo R23 de la Decisión 768/2008.

(66) En consonancia con la noción comúnmente establecida de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, conviene que, cada vez que se produzca un cambio que pueda afectar al cumplimiento de un sistema de IA de alto riesgo por su parte del presente Reglamento (por ejemplo, cambio del sistema operativo o de la arquitectura de software), o cada vez que cambie la finalidad prevista del sistema, dicho sistema de IA se considere un sistema nuevo de IA que debe someterse a una nueva evaluación de la conformidad. Sin embargo, los cambios que se produzcan en el algoritmo y en 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 el modo en que desempeñan sus funciones) no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido predeterminados por el proveedor y se hayan evaluado en el momento de la evaluación de la conformidad.

(67) Los sistemas de IA de alto riesgo deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(68) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas y para la sociedad en su conjunto. Por consiguiente, resulta oportuno que los Estados miembros puedan autorizar, por motivos excepcionales de seguridad pública o con vistas a proteger la vida y la salud de personas físicas y la propiedad industrial y mercantil, 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.

(69) Con el objetivo de facilitar la labor de la Comisión y de los Estados miembros en el ámbito de la inteligencia artificial, así como de incrementar la transparencia de cara al público, debe exigirse a los proveedores de sistemas de IA de alto riesgo que no están asociados a productos que entran dentro del ámbito de aplicación de la legislación de armonización vigente en la Unión que se registren y que registren información sobre dichos sistemas en una base de datos de la UE, de cuya creación y gestión se encargará la Comisión. Antes de utilizar un sistema de IA de alto riesgo enumerado en el anexo III, los usuarios de sistemas de IA de alto riesgo que sean autoridades, agencias u organismos públicos, con excepción de las autoridades encargadas de la aplicación de la ley, del control fronterizo, de la inmigración o del asilo, y de las autoridades que sean usuarios de sistemas de IA de alto riesgo en el ámbito de las infraestructuras críticas también se registrarán en dicha base de datos y seleccionarán el sistema que tengan previsto utilizar. La Comisión debe ser la responsable del tratamiento de dicha base de datos, de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[26]. Con vistas a garantizar la funcionalidad plena de la base de datos una vez que esté en funcionamiento, el procedimiento para su establecimiento debe incluir la elaboración de especificaciones funcionales por parte de la Comisión y la redacción de un informe de auditoría independiente.

[26] 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).

(70) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden conllevar riesgos específicos de suplantación o falsificación, con independencia de si son clasificados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto, en determinadas circunstancias, a obligaciones de transparencia específicas, sin perjuicio de los requisitos y las obligaciones aplicables a los sistemas de IA de alto riesgo. En particular, es preciso notificar a las personas físicas que están interactuando con un sistema de IA, salvo que sea evidente desde el punto de vista de una persona física normalmente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de uso. Al aplicar dicha obligación, las características de las personas pertenecientes a grupos vulnerables debido a su edad o discapacidad deben tenerse en cuenta en la medida en que el sistema de IA esté destinado a interactuar también con dichos grupos. Además, es preciso notificar a las personas físicas 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. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de ojos, los tatuajes, los rasgos personales, el origen étnico, las preferencias e intereses personales o a otros aspectos como la orientación sexual o política. Esta información y estas notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad. Además, los usuarios que utilicen un sistema de IA para generar o manipular imágenes, archivos de audio o vídeos que se asemejen notablemente a personas, lugares o sucesos reales y puedan inducir erróneamente a una persona a pensar que son auténticos, deben comunicar que estos han sido creados o manipulados de manera artificial etiquetando el contenido generado por la inteligencia artificial como corresponda e indicando su origen artificial. El cumplimiento de las obligaciones de información mencionadas no debe interpretarse como indicador de que el uso del sistema o su información de salida sea legal en virtud del presente Reglamento u otra legislación de la Unión o de los Estados miembros, y debe entenderse sin perjuicio de otras obligaciones de transparencia para los usuarios de sistemas de IA establecidas en el Derecho de la Unión o nacional. Tampoco debe interpretarse como indicador de que la utilización del sistema o su información de salida obstaculizan el derecho a la libertad de expresión y el derecho a la libertad de las artes y las ciencias, garantizados en la Carta de los Derechos Fundamentales de la UE, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativo, satírico, artístico o ficticio, con sujeción a unas garantías adecuadas para los derechos y libertades de terceros.

(71) La inteligencia artificial es una familia de tecnologías de rápida evolución que requiere nuevas formas de vigilancia regulatoria y un espacio seguro para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias y medidas de reducción del riesgo adecuadas. Para conseguir un marco jurídico que favorezca la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones, conviene animar a las autoridades nacionales competentes de uno o varios Estados miembros a que establezcan espacios controlados de pruebas para la inteligencia artificial que faciliten el desarrollo y la prueba de sistemas de IA innovadores bajo una estricta vigilancia regulatoria antes de su introducción en el mercado o puesta en servicio.

(72) Los espacios controlados de pruebas para la IA deben tener los objetivos de impulsar la innovación en el ámbito de la IA estableciendo un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización, con vistas a garantizar que los sistemas de IA innovadores cumplan lo dispuesto en el presente Reglamento y en otra legislación pertinente de la Unión y los Estados miembros; de redoblar la seguridad jurídica de que gozan los innovadores y favorecer la vigilancia de las autoridades competentes y su entendimiento de las oportunidades, los riesgos emergentes y las consecuencias del uso de la IA; y de acelerar el acceso a los mercados eliminando las barreras para las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes, entre otras medidas. La participación en el espacio controlado de pruebas para la IA debe centrarse en cuestiones que susciten inseguridad jurídica para que los proveedores y los posibles proveedores innoven, experimenten con la IA en la Unión y contribuyan a un aprendizaje reglamentario basado en pruebas. Por consiguiente, la supervisión de los sistemas de IA en el espacio controlado de pruebas para la IA debe abarcar su desarrollo, entrenamiento, prueba y validación antes de que los sistemas se introduzcan en el mercado o se pongan en servicio, así como la noción y la aparición de modificaciones sustanciales que puedan requerir un nuevo procedimiento de evaluación de la conformidad. Cuando proceda, las autoridades nacionales competentes que establezcan espacios controlados de pruebas para la IA deben cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales, y podrían dar cabida a otros agentes del ecosistema de la IA, como las organizaciones de normalización nacionales o europeas, los organismos notificados, los centros de ensayo y experimentación, los laboratorios de investigación y experimentación, los centros de innovación y las partes interesadas pertinentes y las organizaciones de la sociedad civil. Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas comunes para la creación de espacios controlados de pruebas, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. Los espacios controlados de pruebas para la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otra legislación que permita el establecimiento de otros espacios controlados de pruebas destinados a garantizar el cumplimiento de otra legislación distinta de la del presente Reglamento. Cuando proceda, las autoridades competentes pertinentes encargadas de esos otros espacios controlados de pruebas deben ponderar las ventajas de utilizarlos también con el fin de garantizar el cumplimiento del presente Reglamento por parte de los sistemas de IA. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.

(-72 *bis*) El presente Reglamento debe sentar la base jurídica para que los participantes en el espacio controlados de pruebas para la IA utilicen los datos personales recabados para otros fines en el desarrollo de determinados sistemas de IA en aras del interés público en el espacio controlado de pruebas para la IA, con arreglo al artículo 6, apartado 4, y al artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y a los artículos 5 y 10 del Reglamento (UE) 2018/1725, y sin perjuicio de lo dispuesto en el artículo 4, apartado 2, y el artículo 10 de la Directiva (UE) 2016/680. Siguen siendo aplicables las demás obligaciones de los responsables del tratamiento y los derechos de los interesados en virtud del Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 y la Directiva (UE) 2016/680. En particular, el presente Reglamento no debe servir como fundamento jurídico en el sentido del artículo 22, apartado 2, letra b), del Reglamento (UE) 2016/679 ni del artículo 24, apartado 2, letra b), del Reglamento (UE) 2018/1725. Los participantes en el espacio de pruebas deben proporcionar las salvaguardias adecuadas y cooperar con las autoridades competentes, entre otras cosas, siguiendo sus indicaciones y actuando con rapidez y de buena fe para mitigar cualquier posible alto riesgo para la seguridad y los derechos fundamentales que pueda surgir durante el desarrollo y la experimentación en dicho espacio. Cuando decidan si imponen o no una multa administrativa en virtud del artículo 83, apartado 2, del Reglamento 2016/679 y del artículo 57 de la Directiva 2016/680, las autoridades competentes deben tener en cuenta la conducta de los participantes en el espacio de pruebas.

(72 *bis*) A fin de acelerar el proceso de desarrollo e introducción en el mercado de los sistemas de IA de alto riesgo enumerados en el anexo III, es importante que los proveedores o posibles proveedores de dichos sistemas también puedan beneficiarse de un régimen específico de prueba de dichos sistemas en condiciones reales, sin participar en un espacio controlado de pruebas para la IA. No obstante, en tales casos, y teniendo en cuenta las posibles consecuencias de dichas pruebas para las personas físicas, debe garantizarse que el Reglamento introduzca garantías y condiciones adecuadas y suficientes para los proveedores o posibles proveedores. Estas garantías deben incluir, entre otras cosas, la solicitud del consentimiento informado de las personas físicas para participar en pruebas en condiciones reales, a excepción de la aplicación de la ley en los casos en que la búsqueda del consentimiento informado impida las pruebas del sistema de IA. El consentimiento de los interesados para participar en dichas pruebas en virtud del presente Reglamento es distinto y 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.

(73) Para promover y proteger la innovación, es importante tener en particular consideración los intereses de los proveedores y los usuarios de sistemas de IA que sean pymes. A tal fin, los Estados miembros deben desarrollar iniciativas en materia de concienciación y comunicación de información, entre otros aspectos, dirigidas a dichos operadores. Asimismo, los organismos notificados deben tener en cuenta las necesidades y los intereses específicos de los proveedores que sean pymes cuando establezcan las tasas aplicables a las evaluaciones de la conformidad. Los costes de traducción ligados a la documentación obligatoria y a la comunicación con las autoridades pueden ser considerables para los proveedores y otros operadores, en especial para los de menor tamaño. En la medida de lo posible, los Estados miembros deben procurar que una de las lenguas en las que acepten que los proveedores presenten la documentación pertinente y que pueda usarse para la comunicación con los operadores sea ampliamente conocida por el mayor número posible de usuarios transfronterizos.

(73 *bis*) Con el fin de promover y proteger la innovación, la plataforma de IA a la carta, todos los programas y proyectos de financiación de la UE pertinentes, como el programa Europa Digital, Horizonte Europa, ejecutados por la Comisión y los Estados miembros a nivel nacional o de la UE, deben contribuir a la consecución de los objetivos del presente Reglamento.

(74) En particular, con vistas a reducir al mínimo los riesgos para la aplicación derivados de la falta de conocimientos y experiencia en el mercado, y con el objetivo de facilitar que los proveedores, especialmente las pymes, y los organismos notificados cumplan las obligaciones que les impone el presente Reglamento, la plataforma de IA a la carta, los centros de innovación digital europeos y los centros de ensayo y experimentación establecidos por la Comisión y los Estados miembros a escala nacional o de la UE deben, en la medida de lo posible, contribuir a la aplicación de este Reglamento. En concreto, pueden proporcionar asistencia técnica y científica a los proveedores y organismos notificados en sus respectivas misiones y esferas de competencia.

(74 *bis*) Además, con el fin de garantizar la proporcionalidad, teniendo en cuenta el tamaño muy pequeño de algunos operadores en lo que respecta a los costes de innovación, conviene que las microempresas estén exentas de las obligaciones más costosas, como el establecimiento de un sistema de gestión de la calidad que reduzca la carga administrativa y los costes para dichas empresas sin afectar al nivel de protección ni a la necesidad de cumplir los requisitos aplicables a los sistemas de IA de alto riesgo.

(75) Resulta adecuado que la Comisión facilite, en la medida de lo posible, el acceso a los centros de ensayo y experimentación a organismos, grupos o laboratorios que se hayan establecido o acreditado conforme a la legislación de armonización pertinente de la Unión y que realicen tareas en el marco de la evaluación de la conformidad de productos o dispositivos cubiertos por dicha legislación. Tal es el caso de los paneles de expertos, los laboratorios de expertos y los laboratorios de referencia en el ámbito de los productos sanitarios, conforme al Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746.

(76) Debe establecerse un Comité Europeo de Inteligencia Artificial que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. El Comité debe reflejar los diversos intereses del ecosistema de la IA y estar formado por representantes de los Estados miembros. A fin de garantizar la participación de las partes interesadas pertinentes, debe crearse un subgrupo permanente del Comité. Dicho Comité debe encargarse de diversas tareas de asesoramiento. Entre otras cosas, debe emitir dictámenes, recomendaciones, informes de asesoramiento o contribuir a orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, en particular en lo que respecta al cumplimiento, las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar a la Comisión y a los Estados miembros y sus autoridades nacionales competentes en cuestiones específicas vinculadas a la inteligencia artificial. Con el fin de dar cierta flexibilidad a los Estados miembros en la designación de sus representantes en el Comité de IA, dichos representantes podrán ser personas pertenecientes a entidades públicas que deben tener las competencias y facultades pertinentes para facilitar la coordinación a nivel nacional y contribuir al cumplimiento de las funciones del Comité. El Comité debe crear dos subgrupos permanentes a fin de contar con una plataforma de cooperación e 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. En consonancia con la función y las tareas de la Comisión con arreglo al artículo 33 del Reglamento (UE) 2019/1020, la Comisión debe apoyar las actividades del subgrupo permanente de vigilancia del mercado mediante la realización de evaluaciones o estudios de mercado, en particular con vistas a identificar los aspectos del presente Reglamento que requieran una coordinación específica y urgente entre las autoridades de vigilancia del mercado. El Comité podrá establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. El Comité también debe cooperar, según proceda, con los organismos, grupos de expertos y redes pertinentes de la UE activos en el contexto de la legislación pertinente de la UE, incluidos, en particular, los activos en virtud de la normativa pertinente de la UE sobre datos, productos y servicios digitales.

(76 *bis*) La Comisión debe apoyar activamente a los Estados miembros y a los operadores en la aplicación y el cumplimiento del presente Reglamento. En este sentido, debe elaborar directrices sobre temas concretos al objeto de facilitar la aplicación del presente Reglamento, prestando al mismo tiempo especial atención a las necesidades de las pymes y las empresas emergentes en los sectores que tengan más probabilidades de verse afectados. Con el fin de apoyar el cumplimiento adecuado y las capacidades de los Estados miembros, deben crearse centros de ensayo de la Unión en el ámbito de la IA y un grupo de expertos pertinentes, que se pondrá a disposición de los Estados miembros.

(77) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución de este Reglamento. En este sentido, cada Estado miembro debe designar a una o varias autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Los Estados miembros podrán decidir designar cualquier tipo de entidad pública para que desempeñe las tareas de las autoridades nacionales competentes en el sentido del presente Reglamento, de conformidad con sus características y necesidades organizativas nacionales específicas.

(78) Todos los proveedores de sistemas de IA de alto riesgo deben contar con un sistema de vigilancia poscomercialización, con vistas a garantizar que puedan tener en cuenta la experiencia con el uso de esos sistemas de cara a mejorar los suyos y el proceso de diseño y desarrollo o de que puedan adoptar las medidas correctoras necesarias en el momento oportuno. Este sistema es también fundamental para asegurar que los posibles riesgos derivados de los sistemas de IA que siguen «aprendiendo» tras su introducción en el mercado o puesta en servicio se aborden de un modo más eficiente y oportuno. En este contexto, también procede exigir a los proveedores que cuenten con un sistema para comunicar a las autoridades pertinentes cualquier incidente grave asociado al uso de sus sistemas de IA.

(79) Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación armonizada de la Unión, debe aplicarse en su totalidad el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento deben disponer de todos los poderes de ejecución previstos 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 objetiva. Aunque la mayoría de los sistemas de IA no están sujetos a requisitos ni 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. Esto 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 manera independiente, cuando el Derecho de la Unión exija dicha independencia.

(79 *bis*) 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 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 de los sistemas de IA que presenten un riesgo para la salud, la seguridad o los derechos fundamentales. El procedimiento aplicable a dichos 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 hayan sido introducidos en el mercado, puestos en servicio o utilizados en violación de las prácticas prohibidas establecidas en el presente Reglamento y a los sistemas de IA que estén disponibles infringiendo las obligaciones de transparencia establecidas en el presente Reglamento y que presenten un riesgo.

(80) La legislación de la Unión relativa a los servicios financieros contiene normas y requisitos en materia de gobernanza interna y gestión de riesgos que las entidades financieras reguladas deben cumplir durante la prestación de dichos servicios, y también cuando utilicen sistemas de IA. Para garantizar la aplicación y ejecución coherentes de las obligaciones previstas en el presente Reglamento, así como de las normas y los requisitos oportunos de la legislación de la Unión relativa a los servicios financieros, se ha de designar a las autoridades encargadas de supervisar y ejecutar dicha legislación como las autoridades competentes encargadas de supervisar la aplicación del presente Reglamento, también de cara a las actividades de vigilancia del mercado, en relación con los sistemas de IA proporcionados o usados por entidades financieras reguladas y supervisadas, a menos que un Estado miembro decida designar a otra autoridad para desempeñar estas tareas de vigilancia del mercado. Dichas autoridades competentes deben disponer de todos los poderes previstos en el presente Reglamento y en el Reglamento (UE) 2019/1020 relativo a la vigilancia del mercado para hacer cumplir los requisitos y obligaciones del presente Reglamento, incluidos los poderes para llevar a cabo nuestras actividades de vigilancia del mercado ex post 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 por la Directiva 2013/36/UE, que participen en el Mecanismo Único de Supervisión (MUS) establecido por el Reglamento n.º 1024/2013 del Consejo, comuniquen sin demora al Banco Central Europeo toda información identificada en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento. Con vistas a aumentar la coherencia entre el presente Reglamento y las normas aplicables a las entidades de crédito reguladas por la Directiva 2013/36/UE del Parlamento Europeo y del Consejo[27], conviene igualmente integrar algunas de las obligaciones procedimentales de los proveedores relativas a la gestión de riesgos, el seguimiento posterior a la comercialización y la documentación en las obligaciones y los procedimientos vigentes con arreglo a la Directiva 2013/36/UE. Para evitar solapamientos, también se deben contemplar excepciones limitadas en relación con el sistema de gestión de la calidad de los proveedores y la obligación de seguimiento impuesta a los usuarios de sistemas de IA de alto riesgo, en la medida en que estas 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 reaseguros y a las sociedades de cartera de seguros con

[27] 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).

arreglo a la Directiva 2009/138/UE (Solvencia II) 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, mecanismos o procesos establecidos con arreglo a la legislación pertinente de la Unión en materia de servicios financieros, a fin de garantizar la coherencia y la igualdad de trato en el sector financiero.

(81) El desarrollo de sistemas de IA que no sean sistemas de IA de alto riesgo conforme a los requisitos estipulados en el presente Reglamento puede favorecer la adopción más amplia de inteligencia artificial fiable en la Unión. Se debe instar a los proveedores de sistemas de IA que no son de alto riesgo a crear códigos de conducta destinados a impulsar la aplicación voluntaria de los requisitos aplicables a los sistemas de IA de alto riesgo, adaptados en función de la finalidad prevista de los sistemas y el menor riesgo planteado. Asimismo, se les debe animar a aplicar, con carácter voluntario, requisitos adicionales relativos, por ejemplo, a la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de sistemas de IA, y la diversidad de los equipos de desarrollo. La Comisión podría formular iniciativas, también de carácter sectorial, encaminadas a facilitar la reducción de las barreras técnicas que obstaculizan el intercambio transfronterizo de datos para el desarrollo de IA, también en relación con la infraestructura de acceso a los datos y a la interoperabilidad semántica y técnica de distintos tipos de datos.

(82) Es importante que los sistemas de IA asociados a productos que el presente Reglamento no considera de alto riesgo y que, por lo tanto, no están obligados a cumplir los requisitos establecidos en él sean, no obstante, seguros una vez introducidos en el mercado o puestos en servicio. Para contribuir a este objetivo, se aplicaría, como red de seguridad, la Directiva 2001/95/CE del Parlamento Europeo y del Consejo[28].

(83) Todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, de conformidad con el Derecho nacional y de la Unión, con vistas a garantizar la cooperación fiable y constructiva de las autoridades competentes en la Unión y a escala nacional.

[28] Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DO L 11 de 15.1.2002, p. 4).

(84) Los Estados miembros deben tomar todas las medidas necesarias para asegurarse de que se apliquen las disposiciones del presente Reglamento, incluso estableciendo sanciones efectivas, proporcionadas y disuasorias para las infracciones que se cometan, dentro del respeto del principio *non bis in idem*. En el caso de ciertas infracciones concretas, los Estados miembros deben tener en cuenta los márgenes y criterios establecidos en el presente Reglamento. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas a las instituciones, las agencias y los organismos de la Unión incluidos en el ámbito de aplicación del presente Reglamento.

(85) Con el objetivo de garantizar que el marco reglamentario pueda adaptarse cuando sea necesario, debe delegarse en la Comisión el poder para adoptar actos previsto en el artículo 290 del TFUE, de modo que pueda modificar la legislación de armonización de la Unión indicada en el anexo II, la lista de sistemas de IA de alto riesgo del anexo III, las disposiciones relativas a la documentación técnica que figuran en el anexo IV, el contenido de la declaración UE de conformidad del anexo V, las disposiciones referentes a los procedimientos de evaluación de la conformidad que figuran en los anexos VI y VII, y las disposiciones que estipulan a qué sistemas de IA de alto riesgo debe aplicarse el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y en la evaluación de la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[29]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación 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 ocupen de la preparación de actos delegados. Dichas consultas y apoyo consultivo también deben llevarse a cabo en el marco de las actividades del Comité de IA y de sus subgrupos.

29 DO L 123 de 12.5.2016, p. 1.

(86) 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) n.º 182/2011 del Parlamento Europeo y del Consejo[30]. Reviste especial importancia que, de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación, cuando se necesiten conocimientos especializados más amplios durante las primeras fases de preparación de los proyectos de actos de ejecución, la Comisión recurra a grupos de expertos, consulte a partes interesadas específicas o lleve a cabo consultas públicas, según proceda. Dichas consultas y apoyo consultivo también deben llevarse a cabo en el marco de las actividades del Comité de IA y de sus subgrupos, en particular la preparación de actos de ejecución relacionados con los artículos 4, 4 *bis* y 6.

(87) Dado que el objetivo del presente Reglamento no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones y efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(87 *bis*) A fin de garantizar la seguridad jurídica, garantizar un período de adaptación adecuado para los operadores y evitar perturbaciones del mercado, en particular garantizando la continuidad del uso de los sistemas de IA, es conveniente que el presente Reglamento se aplique a los sistemas de IA de alto riesgo que hayan sido introducidos en el mercado o puestos en servicio antes de la fecha general de aplicación, únicamente si, a partir de esa fecha, dichos sistemas están sujetos a 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 al concepto de modificación sustancial, que se utiliza únicamente con respecto a los sistemas de IA de alto riesgo tal como se definen en el presente Reglamento.

[30] Reglamento (UE) n.º 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).

(88) El presente Reglamento debe aplicarse a partir del ... [*OP – introdúzcase la fecha indicada en el art. 85*]. No obstante, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad debe estar operativa antes de esa fecha, por lo que las disposiciones relativas a los organismos notificados y la estructura de gobernanza deben ser aplicables a partir del ... [*OP – introdúzcase la fecha correspondiente a tres meses a contar desde la entrada en vigor del presente Reglamento*]. Asimismo, los Estados miembros deben establecer y poner en conocimiento de la Comisión las normas referentes a las sanciones, incluidas las multas administrativas, y asegurarse de que para la fecha de aplicación del presente Reglamento se apliquen de manera adecuada y efectiva. De este modo, las disposiciones relativas a las sanciones deben aplicarse a partir del [*OP – introdúzcase la fecha correspondiente a doce meses a contar desde la entrada en vigor del presente Reglamento*].

(89) El Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos fueron consultados de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725, y emitieron un dictamen sobre […].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1
Objeto

El presente Reglamento establece:

a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial («sistemas de IA») en la Unión;

a) prohibiciones de determinadas prácticas de inteligencia artificial;

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

c) normas armonizadas de transparencia aplicables a determinados sistemas de IA;

d) normas sobre el control del mercado, la vigilancia del mercado y la gobernanza;

e) medidas de apoyo a la innovación.

Artículo 2
Ámbito de aplicación

1. El presente Reglamento es aplicable a:

a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están físicamente presentes o están establecidos en la Unión o en un tercer país;

b) los usuarios de sistemas de IA que estén físicamente presentes o estén establecidos en la Unión;

c) los proveedores y usuarios de sistemas de IA que estén físicamente presentes o estén establecidos en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión;

d) los importadores y distribuidores de sistemas de IA;

e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca comercial;

f) representantes autorizados de los proveedores establecidos en la Unión.

2. A los sistemas de IA clasificados como sistemas de AI de alto riesgo de conformidad con el artículo 6, apartados 1 y 2, relacionados con productos contemplados en la legislación de armonización de la Unión que figura en el anexo II, sección B, únicamente se les aplicará el artículo 84 del presente Reglamento. El artículo 53 se aplicará únicamente en la medida en que los requisitos de los sistemas de IA de alto riesgo establecidos en el presente Reglamento se hayan integrado en la legislación de armonización de la Unión.

3. El presente Reglamento no se aplicará a los sistemas de IA que se introduzcan en el mercado, se pongan en servicio o se utilicen con o sin modificación de dichos sistemas para actividades que no entren en el ámbito de aplicación del Derecho de la Unión ni, en cualquier caso, para actividades militares y relativas a la defensa o la seguridad nacional, con independencia del tipo de entidad que lleve a cabo dichas actividades.

   Además, el presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado ni se pongan en servicio en la Unión, cuando la información de salida se utilice en la Unión para actividades que no entren en el ámbito de aplicación del Derecho de la Unión, ni, en cualquier caso, para actividades militares y relativas a la defensa o la seguridad nacional, con independencia del tipo de entidad que lleve a cabo dichas actividades.

4. El presente Reglamento no se aplicará a las autoridades públicas de terceros países ni a las organizaciones internacionales que entren dentro del ámbito de aplicación de este Reglamento conforme al apartado 1 cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos internacionales con fines de aplicación de la ley y cooperación judicial con la Unión o con uno o varios Estados miembros.

5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II, sección 4, de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo[31] [*que deben sustituirse por las disposiciones correspondientes de la Ley de Servicios Digitales*].

6. El presente Reglamento no se aplicará a los sistemas de IA, incluida su información de salida, desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos.

7. El presente Reglamento no se aplicará a ninguna actividad de investigación y desarrollo relativa a los sistemas de IA.

8. El presente Reglamento no se aplicará a las obligaciones de los usuarios que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal no profesional, excepto el artículo 52.

---

[31] 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).

Artículo 3
Definiciones

A los efectos del presente Reglamento, se entenderá por:

(1) «sistema de inteligencia artificial» o «sistema de IA»: un sistema concebido para funcionar con elementos de autonomía que, a partir de datos e información generados por máquinas o por seres humanos, infiere la manera de alcanzar una serie de objetivos, utilizando para ello estrategias de aprendizaje automático o estrategias basadas en la lógica y el conocimiento, y produce información de salida generada por el sistema, como contenidos (sistemas de inteligencia artificial generativa), predicciones, recomendaciones o decisiones, que influyen en los entornos con los que interactúa el sistema de IA;

1 *bis*) «ciclo de vida de un sistema de IA»: la duración de un sistema de IA, desde su concepción hasta su retirada. Sin perjuicio de las competencias de las autoridades de vigilancia del mercado, dicha retirada puede producirse en cualquier momento de la fase de vigilancia poscomercialización por decisión del proveedor, e implica que el sistema no se podrá seguir utilizando. El ciclo de vida de un sistema de IA también finaliza si el proveedor u otra persona física o jurídica modifica sustancialmente el sistema de IA, en cuyo caso el sistema de IA sustancialmente modificado se considerará un nuevo sistema de IA.

1 *ter*) «sistema de IA de uso general»: un sistema de IA que, con independencia de la manera en la que se introduzca en el mercado o se ponga en servicio, incluido el software de código abierto, ha sido concebido por el proveedor para desempeñar funciones de aplicación general, como el reconocimiento de imágenes y de voz, la generación de audio y vídeo, la detección de patrones, la respuesta a preguntas y la traducción, entre otras. Un sistema de IA de uso general puede utilizarse en una pluralidad de contextos e integrarse en una pluralidad de otros sistemas de IA.

(2) «proveedor»: toda persona física o jurídica, autoridad pública, órgano u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA y lo introduzca en el mercado o lo ponga en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita;

(3) [suprimido];

3 *bis*) «pequeñas y medianas empresas» o «pymes»: empresas que se ajustan a la definición que figura en el anexo de la Recomendación 2003/361/CE de la Comisión sobre la definición de microempresas, pequeñas y medianas empresas;

4) «usuario»: toda persona física o jurídica, incluidas las autoridades públicas, órganos u organismos de otra índole, bajo cuya autoridad se utilice un sistema de IA;

5) «representante autorizado»: toda persona física o jurídica con presencia física o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor;

5 *bis*) «fabricante de productos»: fabricante en el sentido de la legislación de armonización de la Unión que se enumera en el anexo II;

6) «importador»: toda persona física o jurídica con presencia física o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión.

7) «distribuidor»: toda persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión;

8) «operador»: el proveedor, el fabricante de productos, el usuario, el representante autorizado, el importador o el distribuidor;

9) «introducción en el mercado»: la primera comercialización en el mercado de la Unión de un sistema de IA;

10) «comercialización»: todo suministro de un sistema de IA para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, ya se produzca el suministro de manera remunerada o gratuita;

11) «puesta en servicio»: el suministro de un sistema de IA para su primer uso directamente al usuario o para uso propio en la Unión de acuerdo con su finalidad prevista;

12) «finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluido el contexto y las condiciones de uso concretas, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica;

13) «uso indebido razonablemente previsible»: la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas razonablemente previsible;

14) «componente de seguridad de un producto o sistema»: un componente de un producto o un sistema que cumple una función de seguridad para dicho producto o sistema, o cuyo fallo o defecto de 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, de la finalidad prevista y de la correcta utilización de un sistema de IA;

16) «recuperación de un sistema de IA»: toda medida encaminada a conseguir la devolución al proveedor de un sistema de IA puesto a disposición de los usuarios, retirarlo del servicio o desactivar su uso;

17) «retirada de un sistema de IA»: toda medida destinada a impedir la comercialización de un sistema de IA que se encuentra en la cadena de suministro;

18) «funcionamiento de un sistema de IA»: la capacidad de un sistema de IA para alcanzar su finalidad prevista;

19) «evaluación de la conformidad»: el proceso por el que se verifica si se cumplen los requisitos establecidos en el título III, capítulo 2, del presente Reglamento en relación con un sistema de IA de alto riesgo;

20) «autoridad notificante»: la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su seguimiento;

21) «organismo de evaluación de la conformidad»: un organismo independiente que desempeña actividades de evaluación de la conformidad, entre las que figuran la prueba, la certificación y la inspección;

22) «organismo notificado»: un organismo de evaluación de la conformidad designado con arreglo al presente Reglamento y otra legislación de armonización pertinente de la Unión;

23) «modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que afecte al cumplimiento por su parte de los requisitos establecidos en el título III, capítulo 2, del presente Reglamento o que provoque la modificación de la finalidad prevista para la que se ha evaluado al sistema de IA en cuestión. En el caso de los sistemas de IA de alto riesgo que continúen aprendiendo tras su introducción en el mercado o su puesta en servicio, los cambios en el sistema de IA de alto riesgo y su funcionamiento que hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y figuren incluidos en la información recogida en la documentación técnica mencionada en el punto 2, letra f), del anexo IV no constituirán modificaciones sustanciales;

24) «marcado CE de conformidad» o «marcado CE»: un marcado con el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el título III, capítulo 2, o en el artículo 4 *ter* del presente Reglamento y otros actos jurídicos de la Unión aplicables que armonicen las condiciones para la comercialización de productos (la «legislación de armonización de la Unión») y prevean su colocación;

25) «sistema de vigilancia poscomercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recopilar y examinar la experiencia obtenida con el uso de sistemas de IA que introducen en el mercado o ponen en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctora o preventiva que resulte necesaria.

26) «autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020;

27) «norma armonizada»: una norma europea conforme a la definición que figura en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012;

28) «especificación común»: un conjunto de especificaciones técnicas, tal como se definen en el artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012, que proporciona medios para cumplir determinados requisitos establecidos en virtud del presente Reglamento;

29) «datos de entrenamiento»: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;

30) «datos de validación»: los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje, entre otras cosas, para evitar el sobreajuste. El conjunto de datos de validación puede ser un conjunto de datos independiente o formar parte del conjunto de datos de entrenamiento, ya sea como una división fija o variable;

31) «datos de prueba»: los datos usados para proporcionar una evaluación independiente del sistema de IA entrenado y validado, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio;

32) «datos de entrada»: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce la información de salida;

33) «datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos;

34) «sistema de reconocimiento de emociones»: un sistema de IA destinado a detectar o deducir los estados mentales, las emociones o las intenciones de las personas físicas a partir de sus datos biométricos;

35) «sistema de categorización biométrica»: un sistema de IA destinado a asignar a las personas físicas a categorías concretas en función de sus datos biométricos;

36) «sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a personas físicas generalmente a distancia, sin su participación activa, comparando sus datos biométricos con los que figuran en un repositorio de datos de referencia;

37) «sistema de identificación biométrica remota "en tiempo real"»: un sistema de identificación biométrica remota en el que la recogida de los datos biométricos, la comparación y la identificación se producen instantáneamente o casi instantáneamente;

38) [suprimido];

39) «espacio de acceso público»: cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que se hayan definido previamente determinadas condiciones o circunstancias de acceso y con independencia de las posibles restricciones de capacidad;

40) «autoridad encargada de la aplicación de la ley»:

a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o

b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública;

41) «aplicación de la ley»: las actividades realizadas por las autoridades encargadas de la aplicación de la ley, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública;

42) [suprimido];

43) «autoridad nacional competente»: o bien la autoridad notificante o bien la autoridad de vigilancia del mercado. En lo que respecta a los sistemas de IA puestos en servicio o utilizados por las instituciones, órganos y organismos de la UE, el Supervisor Europeo de Protección de Datos desempeñará las responsabilidades que en los Estados miembros corresponden a la autoridad nacional competente y, en su caso, toda referencia en el presente Reglamento a las autoridades nacionales competentes o a las autoridades de vigilancia del mercado se entenderán como referencias al Supervisor Europeo de Protección de Datos.

44) «incidente grave»: todo incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, pueda tener alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o daños graves para su salud,

b) una alteración grave e irreversible de la gestión y 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;

45) «infraestructura crítica»: activo, sistema o parte de un activo o sistema que es necesario para la prestación de un servicio esencial para el mantenimiento de funciones sociales o actividades económicas vitales en el sentido de lo dispuesto en el artículo 2, apartados 4 y 5, de la Directiva.../... relativa a la resiliencia de las entidades críticas;

46) «datos personales»: datos en el sentido de lo dispuesto en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

47) «datos no personales»: datos que no sean datos personales en el sentido de lo dispuesto en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

48) «prueba en condiciones reales»: acción de probar temporalmente y en condiciones reales un sistema de IA con su finalidad prevista, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar información completa y fiable y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente Reglamento. La prueba en condiciones reales de un sistema de IA no se considerará equivalente a la introducción en el mercado o a la puesta en servicio de dicho sistema en el sentido de lo dispuesto en el presente Reglamento, siempre que se cumplan todas las condiciones de los artículos 53 o 54 *bis*;

49) «plan de la prueba en condiciones reales»: documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, la supervisión, la organización y la realización de la prueba en condiciones reales;

50) «sujeto»: a los efectos de la prueba en condiciones reales, una persona física que participa en la prueba en condiciones reales;

51) «consentimiento informado»: la expresión libre y voluntaria de la voluntad de un sujeto de participar en una determinada prueba en condiciones reales, tras haber sido informado de todos los aspectos de la prueba que son pertinentes para que el sujeto decida sobre su participación. En el caso de sujetos menores de edad o incapacitados, dará el consentimiento informado su representante legalmente designado;

52) «espacio controlado de pruebas de IA»: marco específico establecido por una autoridad nacional competente que ofrece a los proveedores y potenciales proveedores de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en condiciones reales cuando proceda, un sistema de IA innovador, con arreglo a un plan específico y durante un tiempo limitado, bajo supervisión normativa.

Artículo 4

Actos de ejecución

A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, por lo que respecta a las estrategias de aprendizaje automático y a las estrategias basadas en la lógica y el conocimiento a que se refiere el artículo 3, punto 1), la Comisión podrá adoptar actos de ejecución para definir los elementos técnicos de dichas estrategias, teniendo en cuenta la evolución tecnológica y del mercado. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

TÍTULO I *BIS*

SISTEMAS DE IA DE USO GENERAL

Artículo 4 bis

Cumplimiento del presente Reglamento por los sistemas de IA de uso general

1. Sin perjuicio de lo dispuesto en los artículos 5, 52, 53 y 69 del presente Reglamento, los sistemas de IA de uso general solo cumplirán los requisitos y obligaciones establecidos en el artículo 4 *ter*.

2. Dichos requisitos y obligaciones se aplicarán con independencia de si el sistema de IA de uso general se introduce en el mercado o se pone en servicio como modelo preentrenado y con independencia de si el usuario del sistema de IA de uso general debe realizar ajustes adicionales del modelo.

Artículo 4 ter

Requisitos de los sistemas de IA de uso general y obligaciones de los proveedores de dichos sistemas

1. Los sistemas de IA de uso general que pueden utilizarse como sistemas de IA de alto riesgo o como componentes de sistemas de IA de alto riesgo en el sentido de lo dispuesto en el artículo 6 cumplirán los requisitos establecidos en el título III, capítulo 2, del presente Reglamento a partir de la fecha de aplicación de los actos de ejecución adoptados por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2, a más tardar dieciocho meses después de la entrada en vigor del presente Reglamento. Dichos actos de ejecución especificarán y adaptarán la aplicación de los requisitos establecidos en el título III, capítulo 2, a los sistemas de IA de uso general a la luz de sus características, su viabilidad técnica, las particularidades de la cadena de valor de la IA y la evolución tecnológica y del mercado. Para el cumplimiento de los citados requisitos, se tendrá en cuenta el estado de la técnica generalmente reconocido.

2. Los proveedores de sistemas de IA de uso general a que se refiere el apartado 1 cumplirán, a partir de la fecha de aplicación de los actos de ejecución a que se refiere el apartado 1, las obligaciones establecidas en los artículos 16 *bis bis*, 16 *sexies*, 16 *septies*, 16 *octies*, 16 *decies*, 16 *undecies*, 25, 48 y 61.

3. A los efectos del cumplimiento de las obligaciones establecidas en el artículo 16 *sexies*, los proveedores seguirán el procedimiento de evaluación de la conformidad fundamentado en un control interno establecido en el anexo VI, puntos 3 y 4.

4. Los proveedores de dichos sistemas también mantendrán la documentación técnica a que se refiere el artículo 11 a disposición de las autoridades nacionales competentes por un período de diez años a contar desde la introducción del sistema de IA de uso general en el mercado de la Unión o su puesta en servicio en la Unión.

5. Los proveedores de sistemas de IA de uso general cooperarán con otros proveedores que pretendan poner en servicio o introducir tales sistemas en el mercado de la Unión como sistemas de IA de alto riesgo o como componentes de sistemas de IA de alto riesgo, y les facilitarán la información necesaria, a fin de que esos otros proveedores puedan cumplir las obligaciones que les impone el presente Reglamento. Dicha cooperación entre proveedores preservará, según proceda, los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de conformidad con el artículo 70. A fin de garantizar condiciones uniformes de ejecución del presente Reglamento por lo que respecta a la información que deben proporcionar los proveedores de sistemas de IA de uso general, la Comisión podrá adoptar actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

6. En el cumplimiento de los requisitos y obligaciones a que se refieren los apartados 1, 2 y 3:

- se entenderá que toda referencia a la finalidad prevista es una referencia al posible uso de los sistemas de IA de uso general como sistemas de IA de alto riesgo o como componentes de sistemas de IA de alto riesgo en el sentido de lo dispuesto en artículo 6;

- se entenderá que cuando se haga referencia a los requisitos de los sistemas de IA de alto riesgo del capítulo II, título III, se está haciendo referencia únicamente a los requisitos establecidos en el presente artículo.

Artículo 4 quater
Excepciones al artículo 4 ter

1. El artículo 4 *ter* no se aplicará cuando el proveedor haya excluido expresamente todos los usos de alto riesgo en las instrucciones de uso o en la información que acompaña al sistema de IA de uso general.

2. Dicha exclusión se hará de buena fe y no se considerará justificada si el proveedor tiene motivos suficientes para considerar que el sistema será objeto de un uso indebido.

3. Cuando el proveedor detecte o sea informado de un uso indebido en el mercado, adoptará todas las medidas que sean necesarias y proporcionadas para evitar que se siga llevando a cabo ese uso indebido, en particular teniendo en cuenta la magnitud del uso indebido y la gravedad de los riesgos asociados.

TÍTULO II

PRÁCTICAS DE INTELIGENCIA ARTIFICIAL PROHIBIDAS

Artículo 5

1. Estarán prohibidas las siguientes prácticas de inteligencia artificial:

a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona con el objetivo de alterar de manera sustancial su comportamiento de un modo que provoque o sea razonablemente probable que provoque perjuicios físicos o psicológicos a esa persona o a otra, o que tenga ese efecto.

b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con el objetivo de alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea razonablemente probable que provoque perjuicios físicos o psicológicos a esa persona o a otra, o que tenga ese efecto.

c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a las personas físicas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas físicas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas físicas que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

d) El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público por las autoridades encargadas de la aplicación de la ley, o en su nombre, con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de posibles víctimas concretas de un delito;

ii) la prevención de una amenaza específica e importante para las infraestructuras críticas, la vida, la salud o la seguridad física de las personas físicas o la prevención de un atentado terrorista;

iii) la localización o identificación de una persona física a efectos de una investigación o un enjuiciamiento penales o de la ejecución de sanciones penales por alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo[32] para el que la normativa en vigor en el Estado miembro de que se trate imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, o por algún otro delito específicos para el que la normativa en vigor en el Estado miembro de que se trate imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de cinco años, según determine el Derecho de dicho Estado miembro.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para conseguir cualquiera de los objetivos mencionados en el apartado 1, letra d), tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

[32] 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).

b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra d), cumplirá salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales.

3. Con respecto al apartado 1, letra d), y el apartado 2, cualquier uso de un sistema de identificación biométrica remota «en tiempo real» en un espacio de acceso público con fines de aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema, que la otorgarán previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno mencionadas en el apartado 4. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema sin autorización, siempre que se solicite dicha autorización sin demora indebida mientras se esté utilizando el sistema de IA y que, en caso de que se deniegue la autorización, deje de utilizarse el sistema inmediatamente.

La autoridad judicial o administrativa competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran en el apartado 1, letra d), el cual se indicará en la solicitud. Al pronunciarse al respecto, la autoridad judicial o administrativa competente tendrá en cuenta los aspectos mencionados en el apartado 2.

4. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la notificación relacionadas con estas. Dichas normas especificarán también para cuáles de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen esos sistemas con fines de aplicación de la ley.

TÍTULO III

SISTEMAS DE IA DE ALTO RIESGO

CAPÍTULO 1

CLASIFICACIÓN DE LOS SISTEMAS DE IA COMO SISTEMAS DE ALTO RIESGO

Artículo 6

Reglas de clasificación para los sistemas de IA de alto riesgo

1. Un sistema de IA que constituya en sí mismo un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo II se considerará de alto riesgo si debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos mencionados.

2. Un sistema de IA destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos mencionados en el apartado 1 se considerará de alto riesgo si debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos mencionados. Esta disposición se aplicará aunque el sistema de IA se haya introducido en el mercado o se haya puesto en servicio independientemente del producto.

3. Los sistemas de IA a que se refiere el anexo III se considerarán de alto riesgo salvo que la información de salida del sistema sea meramente accesoria respecto de la acción o decisión pertinente que deba adoptarse y, por tanto, sea poco probable que dé lugar a un riesgo importante para la salud, la seguridad o los derechos fundamentales.

A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, la Comisión adoptará, a más tardar un año después de la entrada en vigor del presente Reglamento, actos de ejecución para especificar las circunstancias en las que la información de salida de los sistemas de IA a que se refiere el anexo III sería meramente accesoria respecto de la acción o decisión pertinente que vaya a adoptarse. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

Artículo 7
Modificaciones del anexo III

1. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar la lista del anexo III mediante la adición de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) los sistemas de IA estén destinados a utilizarse en cualquiera de los ámbitos que figuran en los puntos 1 a 8 del anexo III; y

b) los sistemas de IA conlleven el riesgo de causar un perjuicio a la salud y la seguridad, o el riesgo de tener repercusiones negativas para los derechos fundamentales, cuya gravedad y probabilidad sean equivalentes o mayores a las de los riesgos de perjuicio o de repercusiones negativas asociados a los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando, a los efectos del apartado 1, se evalúe si un sistema de IA conlleva el riesgo de causar un perjuicio a la salud y la seguridad o el riesgo de tener repercusiones negativas para los derechos fundamentales que sea equivalente o mayor a los riesgos de perjuicio asociados a los sistemas de IA de alto riesgo que ya se mencionan en el anexo III, la Comisión tendrá en cuenta los criterios siguientes:

a) la finalidad prevista del sistema de IA;

b) la medida en que se haya utilizado o sea probable que se utilice un sistema de IA;

c) la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas para los derechos fundamentales o haya dado lugar a problemas importantes en relación con la materialización de dicho perjuicio o dichas repercusiones negativas, según demuestren los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes;

d) el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a una gran variedad de personas;

e) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan de la información de salida generada con un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicha información;

f) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del usuario de un sistema de IA, en particular debido a un desequilibrio en cuanto al poder o los conocimientos que ambos poseen, sus circunstancias económicas o sociales, o su edad;

g) la medida en que no sea fácil revertir la información de salida generada con un sistema de IA, habida cuenta de que no se debe considerar que la información de salida que afecta a la salud o la seguridad de las personas es fácil de revertir;

h) la medida en que la legislación vigente en la Unión establezca:

i) medidas de compensación efectivas en relación con los riesgos que conlleva un sistema de IA, con exclusión de las acciones por daños y perjuicios;

ii) medidas efectivas para prevenir o reducir notablemente esos riesgos.

i) la probabilidad de que el uso de la IA resulte beneficioso para las personas, los grupos o la sociedad en general, y la magnitud de este beneficio.

3. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar la lista del anexo III mediante la supresión de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) los sistemas de IA de alto riesgo en cuestión ya no plantean riesgos considerables para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

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

CAPÍTULO 2

REQUISITOS PARA 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 el presente capítulo, teniendo en cuenta el estado de la técnica generalmente reconocido.

2. A la hora de verificar su cumplimiento se tendrán en cuenta la finalidad prevista del sistema de IA de alto riesgo y el sistema de gestión de riesgos al que se refiere el artículo 9.

Artículo 9
Sistema de gestión de riesgos

1. Se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos asociado a los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos se entenderá como un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

   a) la determinación y el análisis de los riesgos conocidos y previsibles más probables en relación con la salud, la seguridad y los derechos fundamentales habida cuenta de la finalidad prevista del sistema de IA de alto riesgo;

   b) [suprimido];

   c) la evaluación de otros riesgos que podrían surgir a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización al que se refiere el artículo 61;

   d) la adopción de medidas oportunas de gestión de riesgos con arreglo a lo dispuesto en los apartados siguientes.

   Los riesgos a que se refiere el presente apartado son únicamente aquellos que pueden mitigarse o eliminarse razonablemente durante el desarrollo o el diseño del sistema de IA de alto riesgo, o mediante el suministro de información técnica adecuada.

3. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), darán la debida consideración a los efectos y la posible interacción derivados de la aplicación combinada de los requisitos estipulados en el presente capítulo 2, con vistas a minimizar los riesgos de manera más eficaz al tiempo que se logra un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo.

A la hora de determinar cuáles son las medidas de gestión de riesgos más adecuadas, se procurará:

a) eliminar o reducir los riesgos detectados y evaluados de conformidad con el apartado 2 en la medida en que sea posible mediante un diseño y un desarrollo adecuados del sistema de IA de alto riesgo;

b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas en relación con los riesgos que no puedan eliminarse;

c) proporcionar la información oportuna conforme al artículo 13, en particular en relación con los riesgos mencionados en el apartado 2, letra b), del presente artículo y, cuando proceda, impartir formación a los usuarios.

Con vistas a eliminar o reducir los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán en la debida consideración los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el usuario, así como el entorno en el que está previsto que se utilice el sistema.

5. Los sistemas de IA de alto riesgo serán sometidos a pruebas a fin de garantizar que dichos sistemas funcionen de manera coherente con su finalidad prevista y cumplan los requisitos establecidos en el presente capítulo.

6. Los procedimientos de prueba podrán incluir pruebas en condiciones reales de conformidad con el artículo 54 *bis*.

7. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en todo caso, antes de su introducción en el mercado o puesta en servicio. Los ensayos se realizarán a partir de parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo de que se trate.

8. El sistema de gestión de riesgos descrito en los apartados 1 a 7 prestará especial atención a la probabilidad de que personas menores de dieciocho años accedan al sistema de IA de alto riesgo o se vean afectadas por él.

9. 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 con arreglo a la legislación sectorial pertinente de la Unión, los aspectos descritos en los apartados 1 a 8 podrán formar parte de los procedimientos de gestión de riesgos establecidos con arreglo a dicha legislación.

Artículo 10
Datos y gobernanza de datos

1. Los sistemas de IA de alto riesgo que utilizan técnicas que implican el entrenamiento de modelos con datos se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad expuestos en los apartados 2 a 5.

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas adecuadas de gobernanza y gestión de datos. Dichas prácticas se centrarán, en particular, en:

   a) la elección de un diseño adecuado;

   b) los procesos de recopilación de datos;

   c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, el enriquecimiento y la agregación;

d) la formulación de los supuestos pertinentes, fundamentalmente en lo que respecta a la información que, ateniéndose a ellos, los datos miden y representan;

e) la evaluación previa de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;

f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas físicas o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión;

g) la detección de posibles lagunas o deficiencias en los datos y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, representativos y en la mayor medida posible, carecerán de errores y estarán completos. Asimismo, tendrán las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema de IA de alto riesgo, cuando proceda. Los conjuntos de datos podrán reunir estas características individualmente para cada dato o para una combinación de estos.

4. Los conjuntos de datos de entrenamiento, validación y prueba tendrán en cuenta, en la medida necesaria en función de su finalidad prevista, las características o elementos particulares del contexto geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la vigilancia, la detección y la corrección de los sesgos asociados a los sistemas de IA de alto riesgo, los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales que se mencionan en 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, ofreciendo siempre las salvaguardias adecuadas para los derechos y las libertades fundamentales de las personas físicas, lo que incluye establecer limitaciones técnicas a la reutilización y la utilización de las medidas de seguridad y protección de la privacidad más recientes, tales como la seudonimización o el cifrado, cuando la anonimización pueda afectar significativamente al objetivo perseguido.

6. Para el desarrollo de sistemas de IA de alto riesgo que no emplean técnicas que implican el entrenamiento de modelos, los apartados 2 a 5 se aplicarán 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 preparará antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada.

   La documentación técnica se redactará de modo que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en el presente capítulo y proporcionará de manera clara y completa a las autoridades nacionales competentes y los organismos notificados toda la información que necesiten para evaluar si el sistema de IA de que se trate cumple dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV o, en el caso de las pymes, incluidas las empresas emergentes, cualquier documentación equivalente que cumpla los mismos objetivos, a menos que la autoridad competente lo considere inadecuado.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto al que se apliquen los actos legislativos mencionados en el anexo II, sección A, se elaborará una única documentación técnica que contenga toda la información estipulada en el anexo IV, así como la información que exijan dichos actos legislativos.

3. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar el anexo IV cuando sea necesario para garantizar que, en vista de los avances técnicos, la documentación técnica proporcione toda la información necesaria para evaluar si el sistema cumple los requisitos establecidos en el presente capítulo.

Artículo 12
Registros

1. Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de eventos («archivos de registro») a lo largo de todo el ciclo de vida del sistema.

2. Para garantizar un nivel de trazabilidad del funcionamiento del sistema de IA que resulte adecuado para la finalidad prevista del sistema, las capacidades de registro permitirán que se registren eventos pertinentes para:

   i) la detección de situaciones que puedan dar lugar a que el sistema de IA presente un riesgo en el sentido del artículo 65, apartado 1, o a una modificación sustancial;

   ii) la facilitación de la vigilancia poscomercialización a que se refiere el artículo 61; y

   iii) el seguimiento del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 29, apartado 4.

4. En el caso de los sistemas de IA de alto riesgo que figuran en el punto 1, letra a), del anexo III, las capacidades de registro incluirán, como mínimo:

   a) un registro del período de cada uso del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización 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 con los que la búsqueda ha arrojado una correspondencia;

   d) la identificación de las personas físicas implicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5.

Artículo 13

Transparencia y comunicación de información a los usuarios

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para lograr el cumplimiento de las obligaciones correspondientes de los usuarios y los proveedores previstas en el capítulo 3 del presente título y permitir que los usuarios comprendan y utilicen adecuadamente el sistema.

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

3. La información a que se refiere el apartado 2 especificará:

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

   b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular:

      i) su finalidad prevista, incluido el entorno geográfico, funcional o de comportamiento específico en el que se pretende utilizar el sistema de IA de alto riesgo;

      ii) el nivel de precisión (incluidos los parámetros para medirla), solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse, así como las circunstancias conocidas y previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado;

      iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista, 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) cuando proceda, su comportamiento con respecto a personas o grupos de personas específicos en los que se pretenda utilizar el sistema;

v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA;

vi) cuando proceda, descripción de la información de salida esperada del sistema;

c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;

d) las medidas de vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios;

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

f) una descripción del mecanismo incluido en el sistema de IA que permite a los usuarios recabar, almacenar e interpretar correctamente los archivos de registro, cuando proceda.

Artículo 14
Vigilancia humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cosas.

2. El objetivo de la vigilancia humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando un sistema de IA de alto riesgo se utiliza conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persisten a pesar de aplicar otros requisitos establecidos en el presente capítulo.

3. La vigilancia humana se garantizará bien mediante uno de los siguientes tipos de medidas, bien mediante todos:

   a) las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio;

   b) las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el usuario.

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1 a 3, el sistema de IA de alto riesgo se ofrecerá al usuario de tal modo que las personas físicas a quienes se encomiende la vigilancia humana puedan, de manera adecuada y proporcionada a estas:

   a) entender las capacidades y limitaciones del sistema de IA de alto riesgo y supervisar debidamente su funcionamiento;

   b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en la información de salida generada por un sistema de IA de alto riesgo («sesgo de automatización»);

   c) interpretar correctamente la información de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;

   d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o desestimar, invalidar o revertir la información de salida que este genere;

   e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema accionando un botón específicamente destinado a tal fin o mediante un procedimiento similar.

5. En el caso de los sistemas de IA mencionados en el punto 1, letra a), del anexo III, las medidas que figuran en el apartado 3 garantizarán, además, que el usuario no actúe ni tome ninguna decisión sobre la base de la identificación generada por el sistema, salvo que un mínimo de dos personas físicas la hayan verificado y confirmado por separado. El requisito de la verificación separada por parte de al menos dos personas físicas no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de aplicación de la ley, de migración, de control fronterizo o de asilo, en los casos en que el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.

Artículo 15
Precisión, solidez y ciberseguridad

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que, en vista de su finalidad prevista, alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en esos sentidos durante todo su ciclo de vida.

2. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión y los parámetros de precisión pertinentes.

3. Los sistemas de IA de alto riesgo serán resistentes a los errores, fallos e incoherencias que pueden surgir en los propios sistemas o en el entorno donde operan, en particular a causa de su interacción con personas físicas u otros sistemas.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.

Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que se elimine o reduzca lo máximo posible el riesgo de que los sesgos que puedan aparecer en la información de salida influyan en la información de entrada de futuras operaciones («bucles de retroalimentación») y se garantice que dichos sesgos se subsanen debidamente con las medidas de mitigación oportunas.

4. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso o funcionamiento aprovechando las vulnerabilidades del sistema.

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

Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («contaminación de datos»), información de entrada diseñada para hacer que el modelo cometa un error («ejemplos adversarios») o los defectos en el modelo.

CAPÍTULO 3

OBLIGACIONES DE LOS PROVEEDORES Y USUARIOS DE SISTEMAS DE IA DE ALTO RIESGO Y DE OTRAS PARTES

Artículo 16
Obligaciones de los proveedores de sistemas de IA de alto riesgo

Los proveedores de sistemas de IA de alto riesgo:

(a) velarán por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en el capítulo 2 del presente título;

a *bis*) indicarán su nombre, su nombre comercial registrado o marca registrada, su dirección de contacto en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, según proceda;

b) contarán con un sistema de gestión de la calidad que cumpla lo dispuesto en el artículo 17;

c) conservarán la documentación a que se refiere el artículo 18;

d) cuando estén bajo su control, conservarán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 20;

e) se asegurarán de que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de la conformidad a que se refiere el artículo 43, antes de su introducción en el mercado o puesta en servicio;

f) cumplirán las obligaciones de registro a que se refiere el artículo 51, apartado 1;

g) adoptarán las medidas correctoras necesarias a que se refiere el artículo 21, cuando el sistema de IA de alto riesgo no sea conforme con los requisitos establecidos en el capítulo 2 del presente título;

h) informarán a la autoridad nacional competente pertinente del Estado miembro donde hayan comercializado o puesto en servicio el sistema de IA y, en su caso, al organismo notificado de los casos de no conformidad y de las medidas correctoras adoptadas;

i) colocarán el marcado CE en sus sistemas de IA de alto riesgo para indicar la conformidad con lo dispuesto en el presente Reglamento, de acuerdo con el artículo 49;

j) demostrarán, previa solicitud de la autoridad nacional competente, la conformidad de sus sistemas de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título.

Artículo 17
Sistema de gestión de la calidad

1. Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema se documentará de manera sistemática y ordenada mediante políticas, procedimientos e instrucciones escritas e incluirá, al menos, los siguientes aspectos:

   a) una estrategia para el cumplimiento reglamentario, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo;

b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo;

c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo y el control y el aseguramiento de la calidad del sistema de IA de alto riesgo;

d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que tendrán lugar;

e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla los requisitos establecidos en el capítulo 2 del presente título;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin;

g) el sistema de gestión de riesgos que se menciona en el artículo 9;

h) el establecimiento, la implantación y el mantenimiento de un sistema de vigilancia poscomercialización con arreglo al artículo 61;

i) los procedimientos asociados a la notificación de un incidente grave con arreglo al artículo 62;

j) la gestión de la comunicación con las autoridades nacionales competentes; las autoridades competentes, incluidas las sectoriales, que permiten acceder a datos o facilitan el acceso a ellos; los organismos notificados; otros operadores; los clientes, u otras partes interesadas;

k) los sistemas y procedimientos destinados a llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluida la seguridad de las medidas relacionadas con el suministro;

m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

2. La inclusión de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor.

2 *bis*. En el caso de los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad con arreglo a la legislación sectorial pertinente de la Unión, los aspectos descritos en el apartado 1 podrán formar parte de los sistemas de gestión de la calidad con arreglo a dicha legislación.

3. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo lo dispuesto en el apartado 1, letras g), h) e i), cuando se respeten las normas relativas a los sistemas o procesos de gobernanza interna de acuerdo con la legislación pertinente de la Unión en materia de servicios financieros. En ese contexto, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40 del presente Reglamento.

Artículo 18
Conservación de la documentación

1. Durante un período que finalizará diez años después de la introducción del sistema de IA en el mercado o su puesta en servicio, el proveedor mantendrá a disposición de las autoridades nacionales competentes:

a) la documentación técnica a que se refiere 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 los cambios aprobados por los organismos notificados, si procede;

d) las decisiones y otros documentos expedidos por los organismos notificados, si procede;

e) la declaración UE de conformidad contemplada en el artículo 48.

1 *bis*. Cada Estado miembro determinará las condiciones en las que la documentación a que se refiere el apartado 1 permanecerá a disposición de las autoridades nacionales competentes durante el período indicado en dicho apartado en los casos en que un proveedor o su representante autorizado establecido en su territorio se declare en quiebra o interrumpa su actividad antes del final de dicho período.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros mantendrán la documentación técnica como parte de la documentación conservada en virtud de la legislación pertinente de la Unión en materia de servicios financieros.

Artículo 19
Evaluación de la conformidad

1. Los proveedores de sistemas de IA de alto riesgo se asegurarán de que sus sistemas sean sometidos al procedimiento oportuno de evaluación de la conformidad, de acuerdo con el artículo 43, antes de su introducción en el mercado o puesta en servicio. Cuando dicha evaluación de la conformidad demuestre que los sistemas de IA cumplen los requisitos establecidos en el capítulo 2 del presente título, sus proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49.

2. [suprimido]

Artículo 20

Archivos de registro generados automáticamente

1. Los proveedores de sistemas de IA de alto riesgo conservarán los archivos de registro a que se refiere el artículo 12, apartado 1, que generen automáticamente sus sistemas de IA de alto riesgo, en la medida en que dichos archivos estén bajo su control en virtud de un acuerdo contractual con el usuario o de conformidad con la ley. Los conservarán durante un período de tiempo de al menos seis meses, salvo que se disponga lo contrario en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros mantendrán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación conservada en virtud de la legislación pertinente en materia de servicios financieros.

Artículo 21

Medidas correctoras

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 investigarán los motivos de inmediato, en su caso, en colaboración con el usuario que haya informado al respecto y adoptarán inmediatamente las medidas correctoras necesarias para que sea conforme, para retirarlo del mercado o para recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo en cuestión y, en su caso, al representante autorizado y a los importadores.

Artículo 22

Obligación de información

Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, y el proveedor del sistema sea consciente de dicho riesgo, dicho proveedor informará de inmediato, en particular sobre el incumplimiento y las medidas correctoras adoptadas, a las autoridades nacionales competentes del Estado miembro donde haya comercializado el sistema y, cuando proceda, al organismo notificado que haya expedido el certificado correspondiente al sistema de IA de alto riesgo.

Artículo 23

Cooperación con las autoridades competentes

Los proveedores de sistemas de IA de alto riesgo proporcionarán a las autoridades nacionales competentes que se lo soliciten toda la información y la documentación necesarias para demostrar la conformidad de sus sistemas de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, en una lengua que pueda entender fácilmente la autoridad del Estado miembro en cuestión. Previa solicitud motivada de una autoridad nacional competente, los proveedores darán a esta acceso a los archivos de registro 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 su control en virtud de un acuerdo contractual con el usuario o de conformidad con la ley.

Artículo 23 bis

Condiciones para que otras personas estén sujetas a las obligaciones de un proveedor

1. Cualquier persona física o jurídica será considerada proveedor de un sistema de IA de alto riesgo a los efectos del presente Reglamento y estará sujeta a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias:

    a) cuando ponga su nombre o marca comercial en un sistema de IA de alto riesgo previamente introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo;

b) [suprimido]

c) cuando haga una modificación sustancial de un sistema de IA de alto riesgo ya introducido en el mercado o puesto en servicio;

d) cuando modifique la finalidad prevista de un sistema de IA que no sea de alto riesgo y que ya haya sido introducido en el mercado o puesto en servicio, de forma que convierta al sistema modificado en un sistema de IA de alto riesgo;

e) cuando introduzca en el mercado o ponga en servicio un sistema de IA de uso general como sistema de IA de alto riesgo o como componente de un sistema de IA de alto riesgo.

2. Cuando se den las circunstancias mencionadas en el apartado 1, letras a) o c), el proveedor que inicialmente haya introducido el sistema de IA de alto riesgo en el mercado o lo haya puesto en servicio dejará de ser considerado proveedor a efectos del presente Reglamento.

3. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos a los que se apliquen los actos jurídicos consignados en el anexo II, sección A, el fabricante de tales productos será considerado proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en alguno de los siguientes supuestos:

i) que el sistema de IA de alto riesgo se introduzca en el mercado junto con el producto bajo el nombre o la marca comercial del fabricante del producto;

ii) que el sistema de IA de alto riesgo se ponga en servicio bajo el nombre o la marca comercial del fabricante del producto después de que este se haya introducido en el mercado.

Artículo 24
[suprimido]

Artículo 25

Representantes autorizados

1. Antes de comercializar sus sistemas en la Unión, los proveedores establecidos fuera de la Unión tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar exclusivamente las tareas siguientes:

-a) verificar que se han elaborado la declaración UE de conformidad y la documentación técnica y que el proveedor ha llevado a cabo un procedimiento adecuado de evaluación de la conformidad;

a) conservar a disposición de las autoridades nacionales competentes y de las autoridades nacionales a que se refiere el artículo 63, apartado 7, durante un período de diez años a partir de la introducción en el mercado o puesta en servicio del sistema de IA de alto riesgo, los datos de contacto del proveedor que haya nombrado al representante autorizado, una copia de la declaración UE de conformidad, la documentación técnica y, en su caso, el certificado expedido por el organismo notificado;

b) proporcionar a una autoridad nacional competente, previa solicitud motivada, toda la información y la documentación, incluida la conservada de acuerdo con la letra b), que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, en particular en lo que respecta al acceso a los archivos de registro a que se refiere el artículo 12, apartado 1, generados automáticamente por ese sistema, en la medida en que dichos archivos estén bajo el control del proveedor en virtud de un acuerdo contractual con el usuario o de conformidad con la ley;

c) cooperar con las autoridades nacionales competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo;

d) cumplir las obligaciones de registro a que se refiere el artículo 51, apartado 1, y, si el propio proveedor lleva a cabo el registro del sistema, verificar que la información a que se refiere el anexo VIII, parte II, puntos 1 a 11, sea correcta.

El representante autorizado pondrá fin al mandato si tiene motivos suficientes para considerar que el proveedor actúa en contra de sus obligaciones en virtud del presente Reglamento. En tal caso, informará asimismo de inmediato a la autoridad de vigilancia del mercado del Estado miembro en el que se encuentre establecido, así como, cuando proceda, al organismo notificado pertinente, de la terminación del mandato y de los motivos de esta medida.

El representante autorizado será legalmente responsable de los sistemas de IA defectuosos sobre la misma base que el proveedor y solidariamente con este con respecto a su posible responsabilidad con arreglo a la Directiva 85/374/CEE del Consejo.

Artículo 26
Obligaciones de los importadores

1. Antes de introducir un sistema de IA de alto riesgo en el mercado, los importadores de dicho sistema se asegurarán de que el sistema sea conforme con el presente Reglamento verificando que:

a) el proveedor de dicho sistema de IA haya llevado a cabo el procedimiento de evaluación de la conformidad pertinente a que se refiere el artículo 43;

b) el proveedor haya redactado la documentación técnica de conformidad con el anexo IV;

c) el sistema lleve el marcado CE de conformidad exigido y vaya acompañado de la declaración UE de conformidad y de las instrucciones de uso;

d) el proveedor haya designado al representante autorizado a que se refiere el artículo 25.

2. Si el importador tiene motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, ha sido falsificado o va acompañado de documentación falsificada, no lo introducirá en el mercado hasta que se haya conseguido la conformidad de dicho sistema. Si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 65, apartado 1, el importador informará de ello al proveedor del sistema de IA, a los representantes autorizados y a las autoridades de vigilancia del mercado.

3. Los importadores indicarán su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, según proceda.

4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán, cuando proceda, de que las condiciones de almacenamiento o transporte no comprometen el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título.

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

5. Los importadores proporcionarán a las autoridades nacionales competentes, previa solicitud motivada, toda la información y la documentación necesarias, incluida la conservada de acuerdo con el apartado 5, para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título en una lengua que dicha autoridad nacional competente pueda entender con facilidad. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades.

5 *bis*. Los importadores cooperarán con las autoridades nacionales competentes en cualquier medida que estas adopten en relación con un sistema de IA del que sean importadores.

Artículo 27

Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE de conformidad exigido, que vaya 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 corresponda, hayan cumplido sus obligaciones previstas en el artículo 16, letra b), y el artículo 26, apartado 3, respectivamente.

2. Si un distribuidor considera o tiene motivos para considerar que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en el capítulo 2 del presente título, no podrá introducirlo en el mercado hasta que se haya conseguido esa conformidad. Del mismo modo, si el sistema presenta un riesgo en el sentido del artículo 65, apartado 1, el distribuidor informará de ello al proveedor o importador del sistema, según corresponda.

3. Mientras sean responsables de un sistema de IA de alto riesgo, los distribuidores se asegurarán, cuando proceda, de que las condiciones de almacenamiento o transporte no comprometen el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título.

4. Los distribuidores que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en el capítulo 2 del presente título adoptarán las medidas correctoras necesarias para que sea conforme, retirarlo del mercado o recuperarlo, o velarán por que el proveedor, el importador u otro operador pertinente, según proceda, adopte dichas medidas correctoras. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 65, apartado 1, su distribuidor informará inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que haya comercializado el producto en cuestión y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad nacional competente, los distribuidores de sistemas de IA de alto riesgo proporcionarán a esta toda la información y la documentación relativa a sus actividades como se describe en los apartados 1 a 4.

5 *bis*. Los distribuidores cooperarán con las autoridades nacionales competentes en cualquier medida que estas adopten en relación con un sistema de IA del que sean distribuidores.

Artículo 28
[suprimido]

Artículo 29
Obligaciones de los usuarios de sistemas de IA de alto riesgo

1. Los usuarios de sistemas de IA de alto riesgo utilizarán dichos sistemas con arreglo a las instrucciones de uso que los acompañen, de acuerdo con los apartados 2 y 5 del presente artículo.

1 *bis*. Los usuarios asignarán la vigilancia humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

2. Las obligaciones previstas en los apartados 1 y 1 *bis* no afectan a otras obligaciones que el Derecho de la Unión o nacional imponga a los usuarios ni a su discrecionalidad para organizar sus propios recursos y actividades con el fin de aplicar las medidas de vigilancia humana que indique el proveedor.

3. Sin perjuicio de lo dispuesto en el apartado 1, el usuario se asegurará de que los datos de entrada sean pertinentes para la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos.

4. Los usuarios pondrán en práctica la vigilancia humana y vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso. Cuando tengan motivos para considerar que utilizar el sistema de IA conforme a sus instrucciones de uso podría hacer que el sistema de IA presente un riesgo en el sentido del artículo 65, apartado 1, informarán al proveedor o distribuidor y suspenderán el uso del sistema. Del mismo modo, si detectan un incidente grave, informarán al proveedor o distribuidor e interrumpirán el uso del sistema de IA. En el caso de que el usuario no consiga contactar con el proveedor, el artículo 62 se aplicará *mutatis mutandis*. Esta obligación no abarcará los datos operativos delicados de los usuarios de sistemas de IA que sean autoridades encargadas de la aplicación de la ley.

En el caso de los usuarios que sean entidades financieras sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de supervisión prevista en el párrafo primero cuando se respeten las normas relativas a los sistemas, procesos y mecanismos de gobernanza interna de acuerdo con la legislación pertinente en materia de servicios financieros.

5. Los usuarios de sistemas de IA de alto riesgo conservarán los archivos de registro a que se refiere el artículo 12, apartado 1, que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Los conservarán durante un período de tiempo de al menos seis meses, salvo que se disponga lo contrario en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

Los usuarios que sean entidades financieras sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros mantendrán los archivos de registro como parte de la documentación conservada en virtud de la legislación pertinente de la Unión en materia de servicios financieros.

5 *bis*. Los usuarios de sistemas de IA de alto riesgo que sean autoridades, agencias u organismos públicos, con excepción de las autoridades encargadas de la aplicación de la ley, del control fronterizo, de inmigración o de asilo, cumplirán las obligaciones de registro a que se refiere el artículo 51. Cuando constaten que el sistema que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 60, no utilizarán dicho sistema e informarán al proveedor o al distribuidor.

6. Los usuarios de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, cuando corresponda.

6 *bis*. Los usuarios cooperarán con las autoridades nacionales competentes en cualquier medida que estas adopten en relación con un sistema de IA del que sean usuarios.

CAPÍTULO 4

AUTORIDADES NOTIFICANTES Y ORGANISMOS NOTIFICADOS

Artículo 30
Autoridades notificantes

1. Cada Estado miembro nombrará o constituirá al menos una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión.

2. Los Estados miembros podrán decidir que la evaluación y la supervisión contempladas en el apartado 1 sean realizadas por un organismo nacional de acreditación en el sentido del Reglamento (CE) n.º 765/2008 y con arreglo a él.

3. Las autoridades notificantes se constituirán, organizarán y operarán de forma que no surjan conflictos de interés con los organismos de evaluación de la conformidad y que se garantice la imparcialidad y objetividad 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 ningún servicio de consultas de carácter comercial o competitivo.

6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida de conformidad con lo dispuesto en el artículo 70.

7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas.

8. [suprimido]

Artículo 31

Solicitud de notificación por parte de un organismo de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación ante 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 sistemas de IA en relación con los cuales 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 33. Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante en virtud de cualquier otra legislación de armonización de la Unión.

3. Si el organismo de evaluación de la conformidad de que se trate no puede facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para verificar, reconocer y supervisar regularmente que cumple los requisitos establecidos en el artículo 33. En lo que respecta a los organismos notificados designados de conformidad con cualquier otra legislación de armonización de la Unión, todos los documentos y certificados vinculados a dichas designaciones podrán utilizarse para apoyar su procedimiento de designación en virtud del presente Reglamento, según proceda. El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 cuando se produzcan cambios pertinentes, para que la autoridad responsable de los organismos notificados pueda supervisar y verificar que se siguen cumpliendo todos los requisitos establecidos en el artículo 33.

Artículo 32
Procedimiento de notificación

1. Las autoridades notificantes solo podrán notificar organismos de evaluación de la conformidad que hayan satisfecho los requisitos establecidos en el artículo 33.

2. Las autoridades notificantes notificarán dichos organismos a la Comisión y a los demás Estados miembros mediante la herramienta de notificación electrónica desarrollada y gestionada por la Comisión.

3. La notificación a que se refiere el apartado 2 incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los sistemas de IA correspondientes, así como la certificación de competencia pertinente. Si la notificación no está basada en el certificado de acreditación a que se refiere el artículo 31, apartado 2, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros las pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones existentes destinadas a garantizar que se controlará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 33.

4. El organismo de evaluación de la conformidad en cuestión únicamente podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no formulan ninguna objeción en el plazo de dos semanas tras la notificación de una autoridad notificante cuando incluya el certificado de acreditación previsto en el artículo 31, apartado 2, o de dos meses tras la notificación de la autoridad notificante cuando incluya las pruebas documentales a que se refiere el artículo 31, apartado 3.

5. [suprimido]

Artículo 33
Requisitos relativos a los organismos notificados

1. Los organismos notificados se establecerán de conformidad con el Derecho nacional y tendrán personalidad jurídica.

2. Los organismos notificados satisfarán los requisitos organizativos, así como los de gestión de la calidad, recursos y procesos, necesarios para el desempeño de sus funciones.

3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados serán tales que ofrezcan confianza en el desempeño y en los resultados de las actividades de evaluación de la conformidad que realicen los organismos notificados.

4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual lleven a cabo actividades de evaluación de la conformidad. Los organismos notificados serán independientes de cualquier otro operador con un interés económico en el sistema de IA de alto riesgo que se evalúe, así como de cualquier competidor del proveedor.

5. Los organismos notificados estarán organizados y gestionados de modo que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán e implantarán una estructura y procedimientos que garanticen la imparcialidad y permitan promover y aplicar los principios de imparcialidad aplicables en toda su organización y a todo su personal y actividades de evaluación.

6. Los organismos notificados se dotarán de procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos respeten la confidencialidad de la información, de acuerdo con el artículo 70, que llegue a su poder en el ejercicio de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija la divulgación de tal información. El personal de los organismos notificados estará sujeto al secreto profesional en lo que respecta a toda la información obtenida en el ejercicio de las tareas encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.

7. Los organismos notificados contarán con procedimientos para desempeñar sus actividades que tengan debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura y el grado de complejidad del sistema de IA de que se trate.

8. Los organismos notificados suscribirán un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que la responsabilidad la asuma el Estado miembro en que estén situados con arreglo a la legislación nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

9. Los organismos notificados serán capaces de llevar a cabo todas las tareas que les competan con arreglo al presente Reglamento con el máximo grado de integridad profesional y la competencia técnica necesaria en el ámbito específico, tanto si dichas tareas las efectúan los propios organismos notificados como si se realizan en su nombre y bajo su responsabilidad.

10. Los organismos notificados contarán con competencias internas suficientes para poder evaluar de manera eficaz las tareas que lleven a cabo agentes externos en su nombre. El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico y científico que tenga experiencia y conocimientos relativos a las tecnologías de inteligencia artificial, los datos y la computación de datos pertinentes y a los requisitos establecidos en el capítulo 2 del presente título.

11. Los organismos notificados participarán en las actividades de coordinación según lo previsto en el artículo 38. Asimismo, tomarán parte directamente o mediante representación en organizaciones europeas de normalización, o se asegurarán de mantenerse al corriente de la situación actualizada de las normas correspondientes.

12. [suprimido]

Artículo 33 bis

Presunción de conformidad con los requisitos relativos a los organismos notificados

Si un organismo de evaluación de la conformidad demuestra su conformidad con los criterios establecidos en las normas armonizadas pertinentes, o en partes de ellas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, se presumirá que cumple los requisitos establecidos en el artículo 33 en la medida en que las normas armonizadas aplicables cubran esos requisitos.

Artículo 34

Filiales de organismos notificados y subcontratación por parte de estos

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 cumplan los requisitos establecidos en el artículo 33 e informará a la autoridad notificante en consecuencia.

2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por los subcontratistas o las filiales con independencia del lugar de establecimiento de estos.

3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor.

4. Los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial, así como el trabajo que estos realicen en virtud del presente Reglamento se mantendrá a disposición de la autoridad notificante durante un período de cinco años a partir de la fecha de finalización de la actividad de subcontratación.

Artículo 34 bis

Obligaciones operativas de los organismos notificados

1. Los organismos notificados verificarán la conformidad de los sistemas de IA de alto riesgo siguiendo los procedimientos de evaluación de la conformidad contemplados en el artículo 43.

2. Los organismos notificados desempeñarán sus actividades evitando cargas innecesarias para los proveedores y teniendo debidamente en cuenta el tamaño de la empresa, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo en cuestión. Para ello, el organismo notificado respetará, sin embargo, el grado de rigor y el nivel de protección requeridos 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 mencionada en el artículo 30, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, que permita que dicha autoridad lleve a cabo sus actividades de evaluación, designación, notificación y seguimiento y facilite la evaluación descrita en el presente capítulo.

Artículo 35

Números de identificación y listas de organismos notificados designados de conformidad con el presente Reglamento

1. La Comisión asignará un número de identificación a cada organismo notificado. Asignará un solo número incluso cuando un organismo sea notificado con arreglo a varios actos de la Unión.

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, junto con los números de identificación que les hayan sido asignados y las actividades para las que hayan sido notificados. La Comisión se asegurará de 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 de la notificación de un organismo notificado a través de la herramienta electrónica de notificación a que se refiere el artículo 32, apartado 2.

2. Los procedimientos descritos en los artículos 31 y 32 se aplicarán a las ampliaciones del alcance de la notificación. Para modificaciones de la notificación distintas de las ampliaciones de su alcance, se aplicarán los procedimientos establecidos en los siguientes apartados.

Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará de ello a la autoridad notificante y a los proveedores afectados tan pronto como sea posible y, cuando se trate de un cese planeado, un año antes de poner fin a sus actividades. Los certificados podrán seguir siendo válidos durante un plazo de nueve meses después del cese de las actividades del organismo notificado, siempre que otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad de los sistemas de IA cubiertos por dichos certificados. El nuevo organismo notificado realizará una evaluación completa de los sistemas de IA afectados al finalizar ese plazo, antes de expedir nuevos certificados para esos sistemas. Si el organismo notificado ha puesto fin a su actividad, la autoridad notificante retirará la designación.

3. Si una autoridad notificante tiene motivos suficientes para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 33 o no está cumpliendo sus obligaciones, dicha autoridad, siempre que el organismo notificado haya tenido la oportunidad de dar a conocer sus puntos de vista, limitará, suspenderá o retirará la notificación, según proceda, dependiendo de la gravedad del incumplimiento de dichos requisitos u obligaciones. Asimismo, informará de ello inmediatamente a la Comisión y a los demás Estados miembros.

4. Cuando su designación haya sido suspendida, limitada o revocada total o parcialmente, el organismo notificado informará a los fabricantes afectados a más tardar en un plazo de diez días.

5. En caso de limitación, suspensión o retirada de una notificación, la autoridad notificante adoptará las medidas oportunas para que los archivos del organismo notificado en cuestión se conserven y se pongan a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado, a petición de estas.

6. En caso de limitación, suspensión o retirada de una designación, la autoridad notificante:

   a) evaluará las repercusiones en los certificados expedidos por el organismo notificado;

   b) presentará a la Comisión y a los demás Estados miembros un informe con sus conclusiones en un plazo de tres meses a partir de la notificación de los cambios en la notificación;

   c) dará instrucciones al organismo notificado para que suspenda o retire, en un plazo razonable determinado por la autoridad, todo certificado indebidamente expedido para garantizar la conformidad de los sistemas de IA en el mercado;

   d) informará a la Comisión y a los Estados miembros de los certificados cuya suspensión o retirada haya exigido;

e) facilitará a las autoridades nacionales competentes del Estado miembro en el que el proveedor tenga su domicilio social toda la información pertinente sobre los certificados para los que haya exigido la suspensión o retirada. Dicha autoridad competente tomará las medidas oportunas, cuando sea necesario, para evitar un riesgo para la salud, la seguridad o los derechos fundamentales.

7. A excepción de los certificados expedidos indebidamente y cuando una notificación haya sido suspendida o limitada, los certificados mantendrán su validez en las circunstancias siguientes:

a) cuando, en el plazo de un mes a partir de la suspensión o la limitación, la autoridad notificante haya confirmado que no existe riesgo alguno para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o la limitación y haya elaborado un calendario y las medidas previstas para poner remedio a la suspensión o la limitación; o

b) cuando la autoridad notificante haya confirmado que no se expedirán, modificarán ni volverán a expedir certificados pertinentes para la suspensión mientras dure la suspensión o limitación, y declare si el organismo notificado tiene o no la capacidad de seguir supervisando y siendo responsable de los certificados existentes expedidos para el período de la suspensión o limitación. En caso de que la autoridad responsable de los organismos notificados determine que el organismo notificado no tiene la capacidad de apoyar los certificados expedidos, el proveedor facilitará a las autoridades nacionales competentes del Estado miembro en que el proveedor del sistema cubierto por el certificado tenga su domicilio social, en el plazo de tres meses a partir de la suspensión o limitación, una confirmación por escrito de que otro organismo notificado cualificado va a asumir temporalmente las funciones del organismo notificado para supervisar los certificados y ser responsable de ellos durante el período de la suspensión o limitación.

8. Salvo para los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados seguirán siendo válidos durante nueve meses, en las circunstancias siguientes:

a) cuando la autoridad nacional competente del Estado miembro en el que el proveedor del sistema de IA cubierto por el certificado tenga su domicilio social haya confirmado que no existe ningún riesgo para la salud, la seguridad y los derechos fundamentales asociado a los sistemas en cuestión; y

b) otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad inmediata de dichos sistemas y que habrá completado la evaluación de estos en el plazo de doce meses desde la retirada de la designación.

En las circunstancias a que se refiere el párrafo primero, la autoridad nacional competente del Estado miembro en el que el proveedor del sistema cubierto por el certificado tenga su domicilio podrá prorrogar la validez provisional de los certificados por plazos adicionales de tres meses, sin exceder de doce meses en total.

La autoridad nacional competente o el organismo notificado que asuman las funciones del organismo notificado afectado por el cambio de la notificación informarán de ello inmediatamente 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, cuando sea necesario, todos los casos en los que existan razones para dudar de que un organismo notificado cumpla los requisitos establecidos en el artículo 33.

2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación del organismo notificado que corresponda.

3. La Comisión garantizará el tratamiento confidencial de acuerdo con el artículo 70 de toda la información de esa naturaleza recabada en el transcurso de sus investigaciones en virtud del presente artículo.

4. Cuando la Comisión determine que un organismo notificado no cumple o ha dejado de cumplir los requisitos establecidos en el artículo 33, informará a la autoridad notificante de los motivos de dicha determinación y le solicitará que adopte las medidas correctoras necesarias, incluidas la suspensión, limitación o retirada de la designación en caso necesario. Si la autoridad notificante no adopta las medidas correctoras necesarias, la Comisión, mediante actos de ejecución, podrá, suspender, limitar o retirar la notificación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 74, apartado 2.

Artículo 38

Coordinación de los organismos notificados

1. La Comisión se asegurará de que se instaure y se explote convenientemente, en relación con los sistemas de IA de alto riesgo, una adecuada coordinación y cooperación entre los organismos notificados activos en los procedimientos de evaluación de la conformidad en virtud del presente Reglamento, en forma de grupo sectorial de organismos notificados.

2. La autoridad notificante se asegurará de que los organismos por ellos notificados participen en el trabajo de este grupo, directamente o por medio de representantes designados.

Artículo 39

Organismos de evaluación de la conformidad de terceros países

Los organismos de evaluación de la conformidad establecidos en virtud del Derecho de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a desempeñar las actividades de los organismos notificados con arreglo al presente Reglamento, siempre que cumplan los requisitos previstos en el artículo 33.

CAPÍTULO 5

NORMAS, EVALUACIÓN DE LA CONFORMIDAD, CERTIFICADOS, REGISTRO

Artículo 40
Normas armonizadas

1. Se presumirá que los sistemas de IA de alto riesgo o los sistemas de IA de uso general que sean conformes con normas armonizadas, o partes de estas, cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea son conformes con los requisitos establecidos en el capítulo 2 del presente título o, en su caso, con los requisitos establecidos en los artículos 4 *bis* y 4 *ter*, en la medida en que dichas normas prevean estos requisitos.

2. Cuando se dirija una solicitud de normalización a las organizaciones europeas de normalización con arreglo al artículo 10 del Reglamento 1025/2012, la Comisión especificará que las normas deben ser coherentes y claras y estar formuladas de un modo que se propongan alcanzar, en particular, los siguientes objetivos:

   a) garantizar que los sistemas de IA introducidos en el mercado o puestos en servicio en la Unión sean seguros y respeten los valores de la Unión y fortalezcan su autonomía estratégica abierta;

   b) promover la inversión y la innovación en IA, incluso mediante el incremento de la certidumbre jurídica, así como la competitividad y el crecimiento del mercado de la Unión;

   c) fomentar la gobernanza de múltiples partes interesadas, representativa de todas las partes interesadas europeas pertinentes (p. ej., industria, pymes, sociedad civil e investigadores);

   d) contribuir al refuerzo de la cooperación mundial en pro de una normalización en el ámbito de la IA que sea coherente con los valores e intereses de la Unión.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de los esfuerzos que dediquen a cumplir los objetivos referidos anteriormente.

Artículo 41

Especificaciones comunes

1. La Comisión estará facultada para adoptar, previa consulta al Comité de IA a que se refiere el artículo 56, actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2, por los que se establezcan especificaciones técnicas comunes para los requisitos establecidos en el capítulo 2 del presente título, o, en su caso, con los requisitos establecidos en los artículos 4 *bis* y 4 *ter*, siempre que se hayan cumplido las siguientes condiciones:

   a) que no se haya publicado ninguna referencia a normas armonizadas que regulen las pertinentes cuestiones esenciales de seguridad o de derechos fundamentales en el Diario Oficial de la Unión Europea, de conformidad con el Reglamento (UE) 1025/2012;

   b) que la Comisión haya solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento n.º 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en el capítulo 2 del presente título;

   c) que la solicitud a que se refiere la letra b) no haya sido aceptada por ninguna de las organizaciones europeas de normalización o que las normas armonizadas a las que se refiere dicha solicitud no se hayan presentado en el plazo fijado de conformidad con el artículo 10, apartado 1, del Reglamento 1025/2012, o dichas normas no se ajustan a la solicitud.

1 *bis*. 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 del apartado 1.

2. En los primeros preparativos del proyecto de acto de ejecución por el que se establezca la especificación común, la Comisión cumplirá los objetivos a que se refiere el artículo 40, apartado 2, y recabará los puntos de vista de los organismos o grupos de expertos pertinentes establecidos en virtud de la legislación sectorial pertinente de la Unión. Sobre la base de dicha consulta, la Comisión preparará el proyecto de acto de ejecución.

3. Se presumirá que los sistemas de IA de alto riesgo o los sistemas de IA de uso general que sean conformes las especificaciones comunes a que se refiere el apartado 1 son conformes con los requisitos establecidos en el capítulo 2 del presente título o, en su caso, con los requisitos establecidos en los artículos 4 *bis* y 4 *ter*, en la medida en que dichas especificaciones comunes prevean estos requisitos.

4. Cuando las referencias de una norma armonizada se publiquen en el Diario Oficial de la Unión Europea, se derogarán, según proceda, los actos de ejecución a que se refiere el apartado 1 que cubran los requisitos establecidos en el capítulo 2 del presente título o los requisitos establecidos en los artículos 4 *bis* y 4 *ter*.

5. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en el capítulo 2 del presente título o los requisitos establecidos en los artículos 4 *bis* y 4 *ter*, según proceda, informará de ello a la Comisión con una explicación detallada, y la Comisión evaluará dicha información y, en su caso, modificará el acto de ejecución por el que se establece la especificación común en cuestión.

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 o funcional específico en el que esté previsto su uso cumplan los correspondientes requisitos establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo o los sistemas de IA de uso general que hayan sido certificados o para los que se haya expedido una declaración de conformidad con arreglo a un esquema de ciberseguridad en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[33] 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 estos, prevean estos 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 el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título por parte de un sistema de IA de alto riesgo, el proveedor haya aplicado normas armonizadas a que se refiere el artículo 40, o bien, en su caso, especificaciones comunes a que se refiere el artículo 41, el proveedor optará por uno de los procedimientos siguientes:

   a) el procedimiento de evaluación de la conformidad fundamentado en un control interno mencionado en el anexo VI; o

   b) el procedimiento de evaluación de la conformidad fundamentado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, con la participación de un organismo notificado, mencionado en el anexo VII.

   Cuando, al demostrar el cumplimiento de los requisitos establecidos en el capítulo 2 del presente título por parte de un sistema de IA de alto riesgo, el proveedor no haya aplicado las normas armonizadas a que se refiere el artículo 40 o solo las haya aplicado parcialmente, o cuando no existan tales normas armonizadas y no se disponga de especificaciones comunes a que se refiere el artículo 41, el proveedor se atendrá al procedimiento de evaluación de la conformidad establecido en el anexo VII.

[33] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad) (DO L 151 de 7.6.2019, p. 1).

A efectos del procedimiento de evaluación de la conformidad establecido en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema por parte de las autoridades encargadas de la aplicación de la ley, las autoridades de inmigración y asilo, así como las instituciones, los organismos o las agencias de la UE, la autoridad de vigilancia del mercado mencionada en el artículo 63, apartado 5 o 6, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en los puntos 2 a 8 del anexo III y de los sistemas de IA de uso general mencionados en el título I *bis*, los proveedores se atendrán al procedimiento de evaluación de la conformidad fundamentado en un control interno a que se refiere el anexo VI, que no contempla la participación de un organismo notificado.

3. En el caso de los sistemas de IA de alto riesgo a los que sean de aplicación los actos legislativos enumerados en el anexo II, sección A, el proveedor se atendrá a la evaluación de la conformidad pertinente exigida por dichos actos legislativos. Los requisitos establecidos en el capítulo 2 del presente título se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. Asimismo, se aplicarán los puntos 4.3, 4.4, 4.5 y 4.6, párrafo quinto, del anexo VII.

A efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo a dichos actos legislativos dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en el capítulo 2 del presente título, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos dispuestos en el artículo 33, apartados 4, 9 y 10, en el contexto del procedimiento de notificación contemplado en dichos actos legislativos.

Cuando los actos legislativos enumerados en el anexo II, sección A, permitan al fabricante del producto prescindir de una evaluación de conformidad realizada por terceros, a condición de que el fabricante haya aplicado todas las normas armonizadas que cubran todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado normas armonizadas, o, en su caso, especificaciones comunes a que se refiere el artículo 41, que cubran los requisitos establecidos en el capítulo 2 del presente título.

4. [suprimido]

5. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de actualizar los anexos VI y VII a la luz del progreso técnico.

6. Se otorgan a la Comisión los poderes para adoptar actos delegados que modifiquen los apartados 1 y 2 a fin de someter a los sistemas de IA de alto riesgo mencionados en los puntos 2 a 8 del anexo III al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes de este. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad fundamentado en un control interno contemplado en el anexo VI para prevenir o reducir al mínimo los riesgos para la salud, la seguridad y la protección de los derechos fundamentales que plantean estos sistemas, así como la disponibilidad de capacidades y recursos adecuados por parte de los organismos notificados.

Artículo 44
Certificados

1. Los certificados expedidos por los organismos notificados con arreglo al anexo VII se redactarán en una lengua que las autoridades competentes del Estado miembro en el que esté establecido el organismo notificado puedan comprender fácilmente.

2. Los certificados serán válidos para el período que indican, que no excederá de cinco años. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos renovables no superiores a cinco años, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado será válido mientras el certificado al que complementa sea válido.

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

Artículo 45

Recurso frente a las decisiones de los organismos notificados

Existirá un procedimiento de recurso frente a las decisiones de los organismos notificados.

Artículo 46

Obligaciones de información de los organismos notificados

1. Los organismos notificados informarán a la autoridad notificante:

   a) de cualquier certificado de la Unión de evaluación de la documentación técnica, cualquier suplemento a dichos certificados y las aprobaciones de sistemas de gestión de la calidad expedidos con arreglo a las condiciones establecidas en el anexo VII;

   b) de cualquier denegación, restricción, suspensión o retirada de un certificado de la Unión de evaluación de la documentación técnica o de una aprobación de un sistema de gestión de la calidad expedidos con arreglo a las condiciones establecidas en el anexo VII;

   c) de cualquier circunstancia que afecte al ámbito o a las condiciones de notificación;

   d) de toda solicitud de información sobre las actividades de evaluación de la conformidad que hayan recibido de las autoridades de vigilancia del mercado;

   e) previa solicitud, de las actividades de evaluación de la conformidad realizadas dentro del ámbito de su notificación y de cualquier otra actividad realizada, con inclusión de las actividades transfronterizas y las subcontrataciones.

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

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

b) de los certificados de evaluación de la documentación técnica de la UE o los suplementos a dichos certificados que haya rechazado, retirado, suspendido o restringido de cualquier otro modo, y, previa solicitud, de los certificados o los suplementos a estos que haya expedido.

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

4. Las obligaciones a que se refieren los apartados 1, 2 y 3 se cumplirán según lo dispuesto en el artículo 70.

Artículo 47

Exención del procedimiento de evaluación de la conformidad

1. No obstante lo dispuesto en el artículo 43 y mediante solicitud debidamente motivada, 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 con el fin de proteger la vida y la salud de las personas, el medio ambiente y activos fundamentales de las industrias e infraestructuras. Dicha autorización se concederá para un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, teniendo en cuenta las razones excepcionales que justifiquen la excepción. La conclusión de los procedimientos en cuestión se alcanzará sin demora indebida.

1 *bis*. 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 las personas físicas, las autoridades encargadas del orden público o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización a que se refiere el apartado 1, siempre que dicha autorización se solicite durante o después de la utilización sin demora indebida y que, en caso de denegación de dicha autorización, se suspenda su uso con efecto inmediato y se descarten inmediatamente todos los resultados e informaciones de salida derivados de dicho uso.

2. La autorización a que se refiere el apartado 1 solo 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 establecidos en el capítulo 2 del presente título. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida de conformidad con el apartado 1. Esta obligación no abarcará los datos operativos delicados relativos a las autoridades encargadas de la aplicación de la ley.

3. [suprimido]

4. [suprimido]

5. [suprimido]

6. En el caso de los sistemas de IA de alto riesgo relacionados con productos regulados por la legislación de armonización de la Unión a que se refiere el anexo II, sección A, solo se aplicarán los procedimientos de excepción de evaluación de la conformidad establecidos en dicha legislación.

Artículo 48
Declaración UE de conformidad

1. El proveedor redactará una declaración UE de conformidad escrita o con firma electrónica para cada sistema de IA y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años después de la introducción del sistema de IA en el mercado o su puesta en servicio. En la declaración UE de conformidad se identificará el sistema de IA para el que ha sido redactada. Se entregará una copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes que lo soliciten.

2. En la declaración UE de conformidad constará que el sistema de IA de alto riesgo de que se trate cumple los requisitos especificados en el capítulo 2 del presente título. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a una lengua que puedan comprender fácilmente las autoridades nacionales competentes del Estado o Estados miembros en que se comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sometidos a otra legislación de armonización de la Unión que también requiera una declaración UE de conformidad, se establecerá una única declaración UE de conformidad relativa a todas las legislaciones de la Unión aplicables 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 la propia declaración se refiera.

4. Al redactar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en el capítulo 2 del presente título. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

5. Se otorgan a la Comisión los poderes para adoptar actos delegados con arreglo al artículo 73 al objeto de actualizar el contenido de la declaración UE de conformidad dispuesta en el anexo V con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

Artículo 49
Marcado CE de conformidad

1. El marcado CE de conformidad estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.

2. El marcado CE se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando esto 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 los documentos adjuntos, según proceda.

3. 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 figurará también en todo el material publicitario en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos de marcado CE.

Artículo 50
[suprimido]

Artículo 51
Registro de los operadores pertinentes y de los sistemas de IA de alto riesgo enumeradas en el anexo III

1. Antes de la introducción en el mercado o la puesta en servicio de un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la acción policial, la migración, el asilo y la gestión del control fronterizo, y los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, el proveedor y, en su caso, el representante autorizado se registrarán en la base de datos de la UE a que se refiere el artículo 60. El proveedor o, en su caso, el representante autorizado, registrará también sus sistemas en dicha base de datos.

2. Antes de utilizar un sistema de IA de alto riesgo enumerado en el anexo III, los usuarios de sistemas de IA de alto riesgo que sean autoridades, agencias u organismos públicos, o entidades que actúen en su nombre, se registrarán en la base de datos de la UE a que se refiere el artículo 60 y seleccionarán el sistema que tengan previsto utilizar.

   Las obligaciones establecidas en el párrafo anterior no se aplicarán a las agencias u organismos y autoridades policiales, de control fronterizo, de inmigración o de asilo, ni a las autoridades, agencias u organismos que utilicen os sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, ni a las entidades que actúen en su nombre.

TÍTULO IV

OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y USUARIOS DE DETERMINADOS SISTEMAS DE IA

Artículo 52

Obligaciones de transparencia de los proveedores y usuarios de determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA, excepto en las situaciones en las que esto resulte evidente desde el punto de vista de una persona jurídica que esté razonablemente informada, observadora y circunspecta, dadas las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento de infracciones penales, con sujeción a las correspondientes salvaguardas de los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar una infracción penal.

2. Los usuarios de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica, autorizados por ley para detectar, impedir e investigar infracciones penales, con sujeción a las correspondientes salvaguardias de los derechos y libertades de terceros.

2 *bis*. Los usuarios de un sistema de reconocimiento de emociones informarán del funcionamiento del sistema a las personas físicas expuestas a él. Esta obligación no se aplicará a los sistemas de IA utilizados para el reconocimiento de emociones, autorizados por ley para detectar, impedir e investigar infracciones penales, con sujeción a las correspondientes salvaguardias de los derechos y libertades de terceros.

3. Los usuarios de un sistema de IA que genere o manipule contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultrafalsificación), harán público que el contenido ha sido generado de forma artificial o manipulado.

No obstante lo anterior, no se aplicará lo dispuesto en el párrafo primero cuando el uso esté autorizado por ley para detectar, impedir, investigar y enjuiciar infracciones penales o cuando el contenido forme parte de una obra o programa manifiestamente creativo, satírico, artístico o ficticio, con sujeción a las correspondientes salvaguardias de los derechos y libertades de terceros.

3 *bis*) La información a que se refieren los apartados 1, 2 y 3 se facilitará a personas físicas de modo claro y visible a más tardar con ocasión de la primera interacción o exposición.

4. Lo dispuesto en los apartados 1, 2, 2 *bis*, 3 y 3 *bis* no afectará a los requisitos y obligaciones establecidos en el título III del presente Reglamento y se entenderá sin perjuicio de otras obligaciones de transparencia para los usuarios de sistemas de IA establecidas en el Derecho de la Unión o nacional.

TÍTULO V

MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 53
Espacios controlados de pruebas para la IA

-1 *bis*. Las autoridades nacionales competentes podrán establecer espacios controlados de pruebas para la IA con fines de desarrollo, entrenamiento, prueba y validación de sistemas de IA innovadores bajo la supervisión, la orientación y el apoyo directos de la autoridad nacional competente, antes de que dichos sistemas se introduzcan en el mercado o se pongan en servicio. Estos espacios controlados de pruebas podrán incluir pruebas en condiciones reales supervisadas por las autoridades nacionales competentes.

-1 *ter*) [suprimido]

- 1 *quater* Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes dentro del ecosistema de la IA.

-1 *quinquies*. Lo dispuesto en el presente artículo no afectará a otros espacios controlados de pruebas establecidos en virtud del Derecho nacional o de la Unión, incluso en los casos en que los productos o servicios que se prueben en ellos estén vinculados al uso de sistemas de IA innovadores. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan a esos otros espacios controlados de pruebas y las autoridades nacionales competentes.

1. [suprimido]

1 *bis*. [suprimido]

1 *ter*) El establecimiento de espacios controlados de pruebas para la IA en virtud del presente Reglamento tendrá por objeto contribuir a uno o varios de los siguientes objetivos:

a) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de IA;
b) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los proporcionen pequeñas y medianas empresas (pymes), incluidas las empresas emergentes;
c) mejorar la certidumbre jurídica y contribuir al intercambio de las mejores prácticas mediante la cooperación con las autoridades que participen en el espacio controlado de pruebas para la IA con vistas a garantizar el cumplimiento futuro del presente Reglamento y, en su caso, de otra legislación de la Unión y de los Estados miembros;
d) contribuir a un aprendizaje reglamentario basado en pruebas.

2. [suprimido]

2 *bis*. El acceso a los espacios controlados de pruebas para la IA estará abierto a todo proveedor o posible proveedor de un sistema de IA que cumpla los criterios de admisibilidad y selección a que se refiere el apartado 6, letra a), y que haya sido seleccionado por las autoridades nacionales competentes tras el procedimiento de selección a que se refiere el apartado 6, letra b). Los proveedores o posibles proveedores también podrán presentar solicitudes en asociación con usuarios o con cualquier otro tercero pertinente.

La participación en el espacio controlado de pruebas para la IA se limitará a un período adecuado a la complejidad y la escala del proyecto. Este plazo podrá ser prorrogado por la autoridad nacional competente.

La participación en el espacio controlado de pruebas para la IA se basará en un plan específico de aquellos a que se refiere el apartado 6 del presente artículo, que será acordado entre el participante o participantes y la autoridad o autoridades nacionales competentes, según proceda.

3. La participación en los espacios controlados de pruebas para la IA no afectará a las facultades de supervisión y correctoras de las autoridades que supervisen el espacio de pruebas. Dichas autoridades ejercerán sus competencias de supervisión de manera flexible dentro de los límites de la legislación pertinente, haciendo uso de su facultad discrecional al aplicar disposiciones jurídicas a un proyecto específico de espacio de pruebas para la IA, con el objetivo de apoyar la innovación en IA en la Unión.

Siempre que el participante o participantes respeten el plan del espacio de pruebas y las condiciones de su participación a que se refiere el apartado 6, letra c), y sigan de buena fe las orientaciones proporcionadas por las autoridades, las autoridades no impondrán multas administrativas por infracción de la legislación aplicable de la Unión o de los Estados miembros relativa al sistema de IA supervisado en el espacio de pruebas, incluidas las disposiciones del presente Reglamento.

4. Los participantes seguirán siendo responsables, conforme a la legislación aplicable de la Unión y de los Estados miembros, de cualquier daño causado durante su participación en un espacio controlado de pruebas para la IA.

4 *bis*. A petición del proveedor o posible proveedor del sistema de IA, la autoridad nacional competente facilitará, cuando proceda, una prueba escrita de las actividades llevadas a cabo con éxito en el espacio controlado de pruebas. La autoridad nacional competente también facilitará un informe de salida en el que se detallen las actividades realizadas en el espacio controlado de pruebas y los resultados y enseñanzas correspondientes. Dichas pruebas escritas y dicho informe de salida podrían ser tenidos en cuenta por las autoridades de vigilancia del mercado o los organismos notificados, según proceda, en el contexto de los procedimientos de evaluación de la conformidad o de los controles de vigilancia del mercado.

Con sujeción a las disposiciones de confidencialidad del artículo 70 y con el acuerdo de los participantes en el espacio de pruebas, la Comisión Europea y el Comité de IA estarán autorizados a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones en virtud del presente Reglamento. Si tanto el participante como la autoridad nacional competente están expresamente de acuerdo, el informe de salida podrá hacerse público a través de la plataforma única de información a que se refiere el artículo 55, apartado 3, letra b).

4 *ter*. Los espacios controlados de pruebas para la IA serán concebidos y aplicados de manera que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.

5. Las autoridades nacionales competentes harán públicos unos informes anuales sobre la aplicación de los espacios controlados de pruebas para la IA, que incluirán buenas prácticas, enseñanzas extraídas y recomendaciones acerca de su configuración, y, en su caso, sobre la aplicación del presente Reglamento y otra legislación de la Unión supervisada en el marco del espacio controlado de pruebas. Dichos informes anuales se presentarán al Comité de IA, que hará público un resumen de todas las buenas prácticas, enseñanzas extraídas y recomendaciones. Esta obligación de hacer públicos los informes anuales no abarcará los datos operativos sensibles en relación con las actividades de las autoridades policiales, de control de fronteras, de inmigración o de asilo. La Comisión y el Comité de IA tendrán en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones en virtud del presente Reglamento.

5 *ter*. La Comisión velará por que la información sobre los espacios controlados de pruebas para la IA, incluidos los establecidos en virtud del presente artículo, esté disponible a través de la plataforma única de información a que se refiere el artículo 55, apartado 3, letra b).

6. Las modalidades y condiciones para el establecimiento y el funcionamiento de los espacios controlados de pruebas para la IA en virtud del presente Reglamento se adoptarán mediante actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 74, apartado 2.

Las modalidades y condiciones apoyarán, en la mayor medida posible, la flexibilidad para que las autoridades nacionales competentes establezcan y exploten sus espacios controlados de pruebas para la IA, fomenten la innovación y el aprendizaje reglamentario y tengan especialmente en cuenta las circunstancias y capacidades especiales de las pymes participantes, incluidas las empresas emergentes.

Dichos actos de ejecución incluirán principios fundamentales comunes sobre las siguientes cuestiones:

a) admisibilidad y selección para participar en el espacio controlado de pruebas para la IA;
b) procedimiento para la solicitud, la participación, el seguimiento, la salida y la finalización del espacio controlado de pruebas para la IA, incluidos el plan del espacio de pruebas y el informe de salida;
c) las condiciones aplicables a los participantes.

7. Cuando las autoridades nacionales competentes estudien la autorización de la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA establecido en virtud del presente artículo, acordarán específicamente con los participantes las condiciones de dichas pruebas 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 el fin de garantizar la coherencia de las prácticas en toda la Unión.

Artículo 54

Tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA en aras del interés público en el espacio controlado de pruebas para la IA

1. En el espacio controlado de pruebas para la IA, se podrán tratar datos personales legalmente recopilados con otros fines con el objetivo de completar el desarrollo, las pruebas y la formación de determinados sistemas innovadores de IA en el espacio controlado de pruebas, con arreglo a las siguientes condiciones acumulativas:

   a) que los sistemas innovadores de IA se desarrollen para que una autoridad pública u otra persona física o jurídica de Derecho público o privado proteja un interés público esencial en uno o varios de los siguientes ámbitos:

      i) [suprimido]

      ii) la seguridad y la salud públicas, incluida la prevención, el control y el tratamiento de enfermedades y la mejora de los sistemas sanitarios;

      iii) la protección y mejora de la calidad del medio ambiente, en particular la transición verde, la mitigación del cambio climático y la adaptación a él;

      iv) la sostenibilidad energética, el transporte y la movilidad;

      v) la eficiencia y calidad de la administración pública y de los servicios públicos;

      vi) la ciberseguridad y resiliencia de la infraestructura crítica.

   b) que los datos tratados resulten necesarios para cumplir uno o varios de los requisitos contemplados en el título III, capítulo 2, cuando dichos requisitos no puedan cumplirse debidamente mediante el tratamiento de datos anonimizados, sintéticos u otro tipo de datos no personales;

c) que existan mecanismos de seguimiento eficaces para detectar si pueden producirse riesgos elevados para los derechos y las libertades de los interesados, tal como figura en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, durante la experimentación en el espacio controlado de pruebas, así como mecanismos de respuesta para mitigar sin demora dichos riesgos y, en su caso, detener el tratamiento;

d) que todos los datos personales que se traten en el contexto del espacio controlado de pruebas se encuentren en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control de los participantes y únicamente accesible para las personas autorizadas;

e) que los datos personales tratados no se transmitan o transfieran a terceros ni sean accesibles de ningún otro modo para ellos, cuando dichos terceros no participen en el espacio controlado de pruebas, a menos que dicha divulgación se produzca de conformidad con el Reglamento (UE) 2016/679 o, en su caso, el Reglamento 2018/725, y todos los participantes estén de acuerdo;

f) que el tratamiento de datos personales en el contexto del espacio controlado de pruebas no afecte a la aplicación de los derechos de los interesados tal como se contempla con arreglo al Derecho de la Unión en materia de protección de datos personales, en particular en el artículo 22 del Reglamento (UE) 2016/679 y en el artículo 24 del Reglamento (UE) 2018/1725;

g) que los datos personales tratados en el contexto del espacio controlado de pruebas se protejan mediante medidas técnicas y organizativas adecuadas y se eliminen una vez concluida la participación en dicho espacio o cuando los datos personales lleguen al final de su período de conservación;

h) que los archivos de registro del tratamiento de datos personales en el contexto del espacio controlado de pruebas se conserven mientras dure la participación en el espacio controlado de pruebas, a menos que se contemple lo contrario en el Derecho de la Unión o el Derecho nacional;

i) que se conserve una descripción completa y detallada del proceso y la justificación del entrenamiento, la prueba y la validación del sistema de IA junto con los resultados del proceso de prueba como parte de la documentación técnica a que se refiere el anexo IV;

j) que se publique una breve síntesis del proyecto de IA desarrollado en el espacio controlado de pruebas, junto con sus objetivos y resultados previstos, en el sitio web de las autoridades competentes. Esta obligación no abarcará los datos operativos delicados relativos a las actividades de las autoridades encargadas de la aplicación de la ley, el control fronterizo, la inmigración o el asilo.

1 *bis*. Con objeto de asegurar la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, bajo el control y la responsabilidad de las autoridades encargadas de la aplicación de la ley, el procesamiento de datos personales en espacios controlados de pruebas para la IA se basará en el Derecho de un Estado miembro concreto o en el Derecho de la Unión, y estará sometido a las mismas condiciones acumuladas que se indican en el apartado 1.

2. El apartado 1 se entiende sin perjuicio del Derecho nacional o de la Unión por el que establecen las bases para el procesamiento de datos personales que sean necesarios para el desarrollo, las pruebas y la formación de sistemas innovadores de IA o cualquier otro fundamento jurídico, de conformidad con el Derecho de la Unión sobre la protección de los datos personales.

Artículo 54 bis

Pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. Las pruebas de sistemas de IA en condiciones reales fuera de los espacios controlados de pruebas para la IA podrán ser realizadas por proveedores o posibles proveedores de sistemas de IA de alto riesgo indicados en el anexo III, de conformidad con las disposiciones del presente artículo y con el plan de pruebas en condiciones reales a que se refiere el presente artículo.

Los elementos detallados del plan de pruebas en condiciones reales se especificarán en actos de ejecución adoptados por la Comisión de conformidad con el procedimiento de estudio a que se refiere el artículo 74, apartado 2.

Esta disposición se entiende sin perjuicio del Derecho nacional o de la Unión en materia de pruebas de sistemas de IA de alto riesgo en condiciones reales en relación con productos abarcados por la legislación indicada en el anexo II.

2. Los proveedores o posibles proveedores podrán realizar pruebas de sistemas de IA de alto riesgo indicados en el anexo III en condiciones reales en cualquier momento antes de la introducción en el mercado o la puesta en servicio del sistema de IA por cuenta propia o en colaboración con uno o más posibles usuarios.

3. Las pruebas de sistemas de IA de alto riesgo en condiciones reales con arreglo al presente artículo se entenderán sin perjuicio de la revisión ética que pueda exigirse en el Derecho nacional o de la Unión.

4. Los proveedores o posibles proveedores podrán realizar pruebas en condiciones reales solamente cuando se cumplan todas las condiciones siguientes:

a) el proveedor o posible proveedor ha desarrollado un plan de pruebas en condiciones reales y lo ha presentado a la autoridad de vigilancia del mercado en aquellos Estados miembros en los que se vayan a realizar las pruebas en condiciones reales;

b) las autoridades de vigilancia del mercado en aquellos Estados miembros en los que se vayan a realizar las pruebas en condiciones reales no se han opuesto a las pruebas en un plazo de treinta días tras la presentación;

c) el proveedor o posible proveedor, con la excepción de aquellos de sistemas de IA de alto riesgo indicados en el anexo III, puntos 1, 6 y 7 en los ámbitos de la aplicación de la ley y la gestión de la migración, el asilo y el control fronterizo, así como de sistemas de IA de alto riesgo indicados en el anexo III, punto 2, ha registrado las pruebas en condiciones reales en la base de datos de la UE a que se refiere el artículo 60, apartado 5 *bis*, con un único número de identificación para toda la Unión y la información indicada en el anexo VIII *bis*;

d) el proveedor o posible proveedor que realice las pruebas en condiciones reales tiene sede en la Unión o ha designado un representante legal con sede en la Unión con objeto de realizar las pruebas en condiciones reales;

e) los datos recopilados y procesados con fines de realizar las pruebas en condiciones reales no se transmitirán a países fuera de la Unión a menos que la transmisión y el procesamiento proporcionen salvaguardias equivalentes a aquellas contempladas con arreglo al Derecho de la Unión;

f) las pruebas en condiciones reales no duran más de lo necesario para lograr sus objetivos, y en cualquier caso no más de doce meses;

g) las personas pertenecientes a grupos vulnerables por causa de su edad y discapacidad física o mental cuentan con protección adecuada;

h) [suprimido]

i) cuando un proveedor o posible proveedor organice las pruebas en condiciones reales en cooperación con uno o más posibles usuarios, estos últimos han sido informados de todos los aspectos de las pruebas que resultan pertinentes para su decisión de participar y que han recibido las instrucciones pertinentes sobre cómo usar el sistema de IA a que se refiere el artículo 13; el proveedor o posible proveedor y el usuario o los usuarios alcanzan un acuerdo en el que se detallan sus funciones y responsabilidades con vistas a asegurar el cumplimiento de las disposiciones para las pruebas en condiciones reales con arreglo al presente Reglamento y otra legislación de aplicación de la Unión y los Estados miembros;

j) los sujetos de las pruebas en condiciones reales han proporcionado su consentimiento informado de conformidad con el artículo 54 *ter*, o, en el caso de las autoridades de aplicación de la ley, en casos en que la solicitud de consentimiento informado evitaría que se realizaran las pruebas sobre el sistema de IA, las pruebas en sí y los resultados de las pruebas en las condiciones reales no tendrán un efecto negativo sobre el sujeto;

k) las pruebas en condiciones reales son supervisadas de manera eficaz por el proveedor o posible proveedor y el usuario o usuarios mediante personas con cualificaciones suficientes en el ámbito pertinente y la capacidad, formación y autoridad necesarias para realizar sus tareas;

l) las predicciones, recomendaciones o decisiones del sistema de IA se pueden revertir o desestimar.

5. Cualquier sujeto de las pruebas en condiciones reales, o su representante legalmente designado, según proceda, podrá abandonar las pruebas en cualquier momento retirando su consentimiento informado, sin sufrir por ello perjuicio alguno y sin necesidad de presentar justificación alguna. La retirada del consentimiento informado no afectará a las actividades ya completadas y a la utilización de datos obtenidos a partir del consentimiento informado antes de su retirada.

6. Se informará de cualquier incidente grave que se identifique en el transcurso de las pruebas en condiciones reales a la autoridad de vigilancia del mercado de conformidad con el artículo 62 del presente Reglamento. El proveedor o posible proveedor adoptará medidas de mitigación inmediatas o, en caso de que esto resulte imposible, suspenderá las pruebas en condiciones reales hasta que se produzca dicha mitigación o se le ponga fin de otro modo. El proveedor o posible proveedor establecerá un procedimiento para la rápida recuperación del sistema de IA en caso de que se ponga fin a las pruebas en condiciones reales.

7. El proveedor o posible proveedor informará a la autoridad de vigilancia del mercado en aquellos Estados miembros en los que se realicen las pruebas en condiciones reales sobre la suspensión o la finalización de las pruebas en condiciones reales y sobre los resultados finales.

8. El proveedor o posible proveedor será responsable, conforme a la legislación aplicable de la Unión y de los Estados miembros, de cualquier daño causado durante su participación en las pruebas en condiciones reales.

Artículo 54 ter

Consentimiento informado para participar en pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. A fin de realizar pruebas en condiciones reales con arreglo al artículo 54 *bis*, el sujeto de las pruebas puede otorgar libremente su consentimiento informado antes de su participación en las pruebas y después de haber recibido información concisa, clara, pertinente y comprensible en relación con:

i) la naturaleza y los objetivos de las pruebas en condiciones reales y las posibles molestias derivadas de su participación;

ii) las condiciones bajo las cuales se han de realizar las pruebas en condiciones reales, en particular la duración prevista de la participación del sujeto;

iii) los derechos y garantías del sujeto de ensayo en lo que respecta a la participación, en particular su derecho a negarse a participar y el derecho a abandonar las pruebas en condiciones reales en cualquier momento sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación;

iv) las modalidades para solicitar la reversión o la desestimación de las predicciones, recomendaciones o decisiones del sistema de IA;

v) el número de identificación único para toda la Unión de la prueba en condiciones reales de conformidad con el artículo 54 *bis*, apartado 4 *quater*, y la información de contacto del proveedor o su representante legal del que se pueda obtener más información.

2. El consentimiento informado estará fechado y documentado, y se enviará una copia al sujeto o a su representante legal.

Artículo 55

Medidas de apoyo a los operadores, concretamente a las pymes, en particular las empresas emergentes

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionar a las pymes, en particular a las empresas emergentes un acceso prioritario a los espacios controlados de pruebas para la IA, siempre y cuando cumplan los criterios de admisibilidad y selección;

b) organizar actividades de sensibilización y formación específicas acerca de la aplicación del presente Reglamento, adaptadas a las necesidades de las pymes, en particular las empresas emergentes y, en su caso, las autoridades públicas locales;

c) en su caso, establecer un canal específico de comunicación con las pymes, en particular las empresas emergentes y, según proceda, las autoridades públicas locales para proporcionar asesoramiento y responder a preguntas sobre la aplicación del presente Reglamento, en particular en relación con la participación en espacios controlados de pruebas para la IA.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores de pymes, en particular de empresas emergentes, a la hora de fijar las tasas para la evaluación de la conformidad en virtud del artículo 43, y se reducirán dichas tasas en proporción a su tamaño, al tamaño del mercado y a otros indicadores pertinentes.

3. La Comisión adoptará las medidas siguientes:

(a) previa solicitud del Comité de IA, proporcionar plantillas normalizadas para los ámbitos cubiertos por el presente Reglamento;

(b) desarrollar y mantener una plataforma única de información que proporcione información fácil de usar en relación con el presente Reglamento para todos los operadores de la Unión;

(c) organizar campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento;

(d) evaluar y fomentar la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con sistemas de IA.

Artículo 55 bis

Excepciones para operadores específicos

1. Las obligaciones establecidas en el artículo 17 del presente Reglamento no se aplicarán a microempresas con arreglo a la definición que figura en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/CE de la Comisión sobre la definición de microempresas, pequeñas y medianas empresas, siempre que dichas empresas no cuenten con empresas asociadas o vinculadas a tenor del artículo 3 de dicho anexo.

2. El apartado 1 no se entenderá como una exención a dichos operadores de cumplir cualquier otro requisito y obligación que figure en el presente Reglamento, en particular aquellos que figuran en los artículo 9, 61 y 62.

3. Los requisitos y obligaciones para sistemas de IA de uso general que figuran en el artículo 4 *ter* no serán de aplicación a microempresas y a pequeñas y medianas empresas, siempre que dichas empresas no cuenten con empresas asociadas o vinculadas a tenor del artículo 3 del anexo de la Recomendación 2003/361/CE de la Comisión sobre la definición de microempresas, pequeñas y medianas empresas.

TÍTULO II

GOBERNANZA

CAPÍTULO 1

COMITÉ EUROPEO DE INTELIGENCIA ARTIFICIAL

Artículo 56
Constitución y estructura del Comité Europeo de Inteligencia Artificial

1. Se establece un «Comité Europeo de Inteligencia Artificial» (el «Comité»).

2. El Comité estará compuesto de un representante por Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Comisión también asistirá a las reuniones del Comité sin participar en las votaciones.

   El Comité podrá invitar a otras autoridades nacionales, autoridades de la Unión, organismos o expertos a las reuniones en función de cada situación concreta, cuando los temas tratados sean de relevancia para ellos.

2 *bis*. Cada representante será designado por su Estado miembro durante un período de tres años, renovable una vez.

2 *bis bis*. Los Estados miembros se asegurarán de que sus representantes en el Comité:

   i) tengan las competencias y facultades pertinentes en su Estado miembro para contribuir de manera activa a la consecución de las tareas del Comité a que se refiere el artículo 58;

   ii) se designen como punto único de contacto respecto del Comité y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

iii) estén facultados para permitir la coherencia y la coordinación entre las autoridades nacionales competentes en su Estado miembro en relación con la aplicación del presente Reglamento, en particular mediante la recopilación de datos e información pertinentes con vistas a realizar sus tareas en el Comité.

3. Los representantes designados de cada Estado miembro adoptarán el reglamento interno del Comité mediante mayoría de dos tercios.

El reglamento interno establecerá en concreto los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las tareas de la presidencia, las modalidades de votación y la organización de las actividades del Comité y sus subgrupos.

Asimismo, el Comité establecerá un subgrupo permanente que funcionará como plataforma para que las partes interesadas asesoren al consejo de administración en todas las cuestiones relacionadas con la aplicación del presente Reglamento, en particular en la preparación de los actos de ejecución y los actos delegados. A tal fin, se invitará a participar en estos subgrupos a las organizaciones que representen los intereses de los proveedores y usuarios de sistemas de IA, en particular las pymes y las empresas emergentes, así como las organizaciones de la sociedad civil, los representantes de las personas afectadas, los investigadores, las organizaciones de normalización, los organismos notificados, los laboratorios y los centros de ensayo y experimentación. El Comité creará dos subgrupos permanentes a fin de contar con una plataforma de cooperación e 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 Comité podrá establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. En su caso, las partes interesadas a que se refiere el párrafo anterior podrán ser invitadas, en calidad de observadores, a los subgrupos o a reuniones concretas de dichos subgrupos.

3 *bis*) El Comité se organizará y gestionará de manera que se preserve la objetividad e imparcialidad de sus actividades.

4. El Comité estará presidido por uno de los representantes de los Estados miembros. Previa solicitud de la presidencia, la Comisión convocará las reuniones y elaborará el orden del día de conformidad con las funciones del Comité en virtud del presente Reglamento y con su reglamento interno. La Comisión prestará apoyo administrativo y analítico a las actividades del Comité en virtud del presente Reglamento.

Artículo 57
[suprimido]

Artículo 58
Funciones del Comité

El Comité prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la coherencia y la aplicación eficaz del presente Reglamento. A tal fin, el Comité podrá, entre otros:

a) recopilar y compartir conocimientos técnicos y reglamentarios y buenas prácticas entre los Estados miembros;

b) contribuir a la armonización de las prácticas administrativas en los Estados miembros, en particular en relación con la exención de los procedimientos de evaluación de la conformidad a que se refiere el artículo 47, el funcionamiento de espacios controlados de pruebas y ensayos en condiciones reales a que se refieren los artículos 53, 54 y 54 *bis*.

c) previa solicitud de la Comisión o bajo su propia iniciativa, emitir recomendaciones y dictámenes por escrito en relación con cualquier asunto pertinente relacionado con la aplicación del presente Reglamento y con su aplicación coherente y eficaz, en particular:

   i) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el título III, capítulo 2;

   ii) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41;

iii) sobre la preparación de documentos de orientación, incluidas las directrices relativas a la fijación de multas administrativas a que se refiere el artículo 71;

d) proporcionar asesoramiento a la Comisión sobre la posible necesidad de modificar el anexo III de conformidad con los artículos 4 y 7, teniendo en cuenta las pruebas pertinentes disponibles y las novedades en materia tecnológica;

e) proporcionar asesoramiento a la Comisión durante la preparación de actos delegados o de ejecución en virtud del presente Reglamento;

f) cooperar, según proceda, con organismos pertinentes de la UE, grupos de expertos y redes, en particular en los ámbitos de la seguridad alimentaria, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, las criptodivisas, la protección de los consumidores y la protección de los datos y los derechos fundamentales.

g) aportar y proporcionar asesoramiento pertinente a la Comisión en el desarrollo de las directrices a que se refiere el artículo 58 *bis* o solicitar el desarrollo de dichas directrices;

h) con objeto de proporcionar asistencia para la labor de las autoridades de vigilancia del mercado y, en cooperación con las autoridades de vigilancia del mercado interesadas, y previo acuerdo con ellas, fomentar y apoyar las investigaciones transfronterizas de vigilancia del mercado, en particular en relación con la aparición de riesgos de naturaleza sistémica que puedan tener su origen en sistemas de IA;

i) contribuir a la evaluación de necesidades de formación para el personal de los Estados miembros que participe en la aplicación del presente Reglamento;

j) asesorar a la Comisión en relación con asuntos internacionales en materia de inteligencia artificial.

CAPÍTULO 1 *BIS*

DIRECTRICES DE LA COMISIÓN

Artículo 58 bis

Directrices de la Comisión sobre la aplicación del presente Reglamento

1. A petición de los Estados miembros o del Comité, o a iniciativa propia, la Comisión emitirá directrices sobre la aplicación práctica del presente Reglamento, y en concreto sobre:

   i) para la aplicación de los requisitos contemplados en los artículos 8 a 15;

   ii) las prácticas prohibidas a que se refiere el artículo 5;

   iii) la aplicación práctica de las disposiciones relacionadas con las modificaciones sustanciales;

   iv) la aplicación práctica de las condiciones uniformes a que se refiere el artículo 6, apartado 3, en particular los ejemplos de sistemas de IA de alto riesgo a que se refiere el anexo III;

   v) la aplicación práctica de las obligaciones de transparencia que figuran en el artículo 52;

   vi) la relación del presente Reglamento y otra legislación pertinente de la Unión, en particular en relación con la coherencia de su aplicación.

Al emitir estas directrices, la Comisión prestará especial atención a las necesidades de las pymes, en particular las empresas emergentes, y de las autoridades públicas locales y los sectores que más puedan verse afectados por el presente Reglamento.

CAPÍTULO 2

AUTORIDADES NACIONALES COMPETENTES

Artículo 59
Designación de autoridades nacionales competentes

1. [suprimido]

2. Cada Estado miembro establecerá o designará al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a los efectos del presente Reglamento. Estas autoridades nacionales competentes se organizarán de manera que se preserve la objetividad e imparcialidad de sus actividades y funciones. Siempre que se respeten estos principios, estas actividades y tareas podrán ser realizadas por una o varias autoridades designadas, de conformidad con las necesidades organizativas del Estado miembro.

3. Los Estados miembros informarán a la Comisión de su designación o sus designaciones.

4. Los Estados miembros garantizarán que las autoridades nacionales competentes dispongan de recursos financieros, equipos técnicos y recursos humanos con buenas cualificaciones adecuados para el desempeño eficaz de sus funciones con arreglo al presente Reglamento.

5. A más tardar el *[un año después de la entrada en vigor del presente Reglamento]* y posteriormente seis meses antes del plazo que figura en el artículo 84, apartado 2, los Estados miembros informarán a la Comisión acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión transmitirá dicha información al Comité para su debate y la formulación de posibles recomendaciones.

6. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.

7. Las autoridades nacionales competentes podrán proporcionar asesoramiento en relación con la aplicación del presente Reglamento, también adaptada a los proveedores de pymes, en particular las empresas emergentes. Siempre que una autoridad nacional competente pretenda proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otra legislación de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dicha legislación de la Unión, según proceda. Asimismo, los Estados miembros podrán establecer un punto de contacto central para la comunicación con los operadores.

8. Cuando las instituciones, agencias y 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.

TÍTULO VII

BASE DE DATOS DE LA UE PARA SISTEMAS DE IA DE ALTO RIESGO ENUMERADOS EN EL ANEXO III

Artículo 60

Base de datos de la UE para 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 contendrá la información prevista en el apartado 2 en relación con los operadores pertinentes y los sistemas de IA de alto riesgo enumerados en el anexo III que están registrados con arreglo a los artículos 51 y 54 *bis*. La Comisión consultará al Comité de la IA al fijar las especificaciones funcionales de dicha base de datos.

2. Los datos enumerados en el anexo III, parte I, serán introducidos en la base de datos de la UE por los proveedores, representantes autorizados y usuarios pertinentes, en su caso, al registrarse. Los datos enumerados en el anexo VIII, parte II, puntos 1 a 11, serán introducidos en la base de datos de la UE por los proveedores o, en su caso, los representantes autorizados, de conformidad con el artículo 51. La datos enumerados en el anexo VIII, parte II, punto 12, serán generados automáticamente por la base de datos a partir de la información proporcionada por usuarios pertinentes en virtud del artículo 51, apartado 2. Los datos enumerados en el anexo VIII *bis* serán introducidos en la base de datos por los proveedores o posibles proveedores de conformidad con el artículo 54 *bis*.

3. [suprimido]

4. La base de datos de la UE no contendrá datos personales, con la excepción de la información enumerada en el anexo VIII, y se entenderá sin perjuicio del artículo 70.

5. La Comisión será la responsable del tratamiento de la base de datos de la UE, y proporcionará apoyo técnico y administrativo adecuado a los proveedores, posibles proveedores y usuarios.

5 *bis*. La información presente en la base de datos de la UE y registrada de conformidad con el artículo 51 será accesible para el público. La información registrada de conformidad con el artículo 54 *bis* solo será accesible para las autoridades de vigilancia de mercado y para la Comisión, a menos que el proveedor o posible proveedor haya dado su consentimiento a hacer esta información accesible también para el público.

TÍTULO VIII

VIGILANCIA POSCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN, VIGILANCIA DEL MERCADO

CAPÍTULO 1

VIGILANCIA POSCOMERCIALIZACIÓN

Artículo 61

Vigilancia poscomercialización por parte de los proveedores y plan de vigilancia poscomercialización para sistemas de IA de alto riesgo

1. Los proveedores establecerán y documentarán un sistema de vigilancia poscomercialización de forma proporcionada a los riesgos de los sistemas de IA de alto riesgo.

2. A fin de que el proveedor pueda evaluar si los sistemas de IA cumplen los requisitos establecidos en el título III, capítulo 2, a lo largo de todo su ciclo de vida, el sistema de vigilancia poscomercialización recopilará, documentará y analizará los datos pertinentes que puedan facilitar los usuarios o que puedan recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo. Esta obligación no abarcará los datos operativos delicados de los usuarios de sistemas de IA que sean autoridades encargadas de la aplicación de la ley.

3. El sistema de vigilancia poscomercialización se basará en un plan de vigilancia poscomercialización. El plan de vigilancia poscomercialización formará parte de la documentación técnica a que se refiere el anexo IV. La Comisión adoptará un acto de ejecución en el que se establecerán disposiciones detalladas que constituyan un modelo para el plan de vigilancia poscomercialización y la lista de elementos que deberán incluirse en él.

4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos a que hace referencia el anexo II, sección A, cuando ya se hayan establecido un sistema y un plan de vigilancia poscomercialización con arreglo a dicha legislación, la documentación de vigilancia poscomercialización preparada con arreglo a dicha legislación será considerada suficiente, siempre que se utilice el modelo a que se refiere el apartado 3.

El párrafo primero también se aplicará a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, introducidos en el mercado o puestos en servicio por entidades financieras sujetas a requisitos en materia de gobernanza interna, mecanismos o procesos establecidos con arreglo a la legislación de la Unión en materia de servicios financieros.

CAPÍTULO 2

INTERCAMBIO DE INFORMACIÓN SOBRE INCIDENTES GRAVES

Artículo 62
Notificación de incidentes graves

1. Los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión notificarán cualquier incidente grave a las autoridades de vigilancia del mercado de los Estados miembros donde se haya producido dicho incidente.

Dicha notificación se efectuará inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la posibilidad razonable de que exista dicho vínculo, y, en cualquier caso, a más tardar quince días después de que los proveedores tengan conocimiento de dicho incidente grave.

2. Tras la recepción de la notificación relativa al incidente grave a que se refiere el artículo 3, punto 44, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 64, apartado 3. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1. Dichas orientaciones se publicarán en el plazo máximo de doce meses tras la entrada en vigor del presente Reglamento.

3. En el caso de los sistemas de IA de alto riesgo a que se refiere el punto 5 del anexo III introducidos en el mercado o puestos en servicio por proveedores que sean entidades financieras sujetas a requisitos en materia de gobernanza interna, mecanismos o procesos establecidos con arreglo a la legislación de la Unión en materia de servicios financieros, la notificación de incidentes graves se limitará a los referidos en el artículo 3, punto 44, letra c).

4. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de dispositivos, o que en sí mismos sean dispositivos, regulados por el Reglamento (UE) 2017/745 y el Reglamento (UE) 2017/746, la notificación de incidentes graves se limitará a los referidos en el artículo 3, punto 44, letra c), y la hará la autoridad nacional competente elegida para este fin por los Estados miembros en los que se produzca dicho incidente.

CAPÍTULO 3

EJECUCIÓN

Artículo 63

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. No obstante, a efectos de la ejecución eficaz del presente Reglamento:

   a) se entenderá que toda referencia a un operador económico con arreglo al Reglamento (UE) 2019/1020 incluye a todos los operadores identificados en el artículo 2 del presente Reglamento;

   b) se entenderá que toda referencia a un producto con arreglo al Reglamento (UE) 2019/1020 incluye todos los sistemas de IA que estén comprendidos en el ámbito de aplicación del presente Reglamento.

2. Como parte de sus obligaciones de presentación de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado informarán a la Comisión de los resultados de las actividades de vigilancia del mercado pertinentes en virtud del presente Reglamento.

3. En el caso de los sistemas de IA de alto riesgo relacionados con productos a los que sean de aplicación los actos legislativos enumerados en el anexo II, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designadas en virtud de dichos actos legislativos o, en circunstancias justificadas y siempre que se garantice la coordinación, otra autoridad pertinente identificada por el Estado miembro.

   Los procedimientos a que se refieren los artículos 65, 66, 67 y 68 del presente Reglamento no se aplicarán a los sistemas de IA relacionados con productos a los que se apliquen los actos jurídicos que figuran en el anexo II, sección A, cuando dichos actos jurídicos ya prevean procedimientos que tengan el mismo objetivo. En dicho caso, se aplicarán en su lugar estos procedimientos sectoriales.

4. En el caso de los sistemas de IA de alto riesgo introducidos en el mercado, puestos en servicio o utilizados por entidades financieras reguladas por la legislación de la Unión sobre 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 la mencionada legislación, en la medida en que la introducción en el mercado, la puesta en servicio o la utilización del sistema de IA esté directamente relacionada con la prestación de dichos servicios financieros.

   Como excepción a lo dispuesto en el párrafo anterior, en circunstancias justificadas y siempre que se garantice la coordinación, el Estado miembro podrá designar otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.

   Las autoridades nacionales de vigilancia del mercado que supervisen las entidades de crédito reguladas por la Directiva 2013/36/UE y que participen en el Mecanismo Único de Supervisión (MUS) establecido por el Reglamento n.º 1204/2013 del Consejo, deberán comunicar sin demora al Banco Central Europeo toda información identificada en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

5. En el caso de los sistemas de IA de alto riesgo enumerados en el punto 1, letra a), en la medida en que los sistemas se utilicen a los efectos de la aplicación de la ley, y en los puntos 6, 7 y 8 del anexo III, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades nacionales responsables de supervisar las actividades de las autoridades encargadas de la aplicación de la ley, del control de fronteras, de la inmigración o del asilo o de las autoridades judiciales, o bien a las autoridades de control encargadas de la protección de datos con arreglo a la Directiva (UE) 2016/680 o al Reglamento 2016/679. 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 en el ejercicio de su función judicial.

6. Cuando las instituciones, agencias y 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.

7. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento y otras autoridades u organismos nacionales pertinentes responsables de supervisar la aplicación de la legislación de armonización de la Unión citada en el anexo II u otra legislación de la Unión que pueda resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

8. 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 tareas, el proveedor concederá a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo del sistema de IA de alto riesgo, también, cuando proceda y con sujeción a salvaguardias de seguridad, a través de interfaces de programación de aplicaciones (API) u otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

9. Se concederá acceso a las autoridades de vigilancia del mercado al código fuente del sistema de IA de alto riesgo, previa solicitud motivada y solo si se cumplen las siguientes condiciones acumulativas:

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 el título III, capítulo 2, y

b) los procedimientos y verificaciones de prueba/auditoría basados en los datos y la documentación facilitados por el proveedor se han agotado o han resultado insuficientes.

10. Cualquier información y documentación obtenidas por las autoridades de vigilancia del mercado se tratarán de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 70.

11. Cualquier persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones a la autoridad de vigilancia del mercado pertinente.

De conformidad con el artículo 11, apartado 3, letra e), y el artículo 11, apartado 7, letra a), del Reglamento (UE) 2019/1020, las reclamaciones se tendrán en cuenta a la hora de llevar a cabo las actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos, por tanto, por las autoridades de vigilancia del mercado.

Artículo 63 bis

Supervisión de las pruebas en condiciones reales por parte de las autoridades de vigilancia del mercado

1. Las autoridades de vigilancia del mercado tendrán la competencia y los poderes necesarios para garantizar que las pruebas en condiciones reales se ajusten a lo dispuesto en el presente Reglamento.

2. Cuando se realicen pruebas en condiciones reales de sistemas de IA supervisados dentro de un espacio controlado de pruebas para la IA con arreglo al artículo 54, las autoridades de vigilancia del mercado verificarán el cumplimiento de lo dispuesto en el artículo 54 *bis* como parte de su función supervisora del espacio controlado de pruebas para la IA. Dichas autoridades podrán permitir, según proceda, que el proveedor o posible proveedor lleve a cabo las pruebas en condiciones reales, como excepción a las condiciones establecidas en el artículo 54 *bis*, apartado 4, letras f) y g).

3. Cuando el posible proveedor, el proveedor o un tercero informe a la autoridad de vigilancia del mercado de un incidente grave o tenga motivos para pensar que las condiciones establecidas en los artículos 54 *bis* y 54 *ter* no se cumplen, podrá adoptar cualquiera de las decisiones siguientes en su territorio, según proceda:

a) suspender o poner fin a las pruebas en condiciones reales;

b) exigir al proveedor o posible proveedor y al usuario o usuarios que modifiquen cualquier aspecto de la prueba en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión con arreglo al apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 54 *bis*, apartado 4, letra b), la decisión o la objeción deberá estar motivada e indicar las modalidades y condiciones en las 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 la decisión a que se refiere el apartado 3 del presente artículo, comunicará los motivos de la misma a las autoridades de vigilancia del mercado de los demás Estados miembros en los que el sistema de IA haya sido sometido a pruebas de conformidad con el plan de prueba.

Artículo 64

Competencias de las autoridades encargadas de proteger los derechos fundamentales

1. [suprimido]

2. [suprimido]

3. Las autoridades u organismos públicos nacionales encargados de supervisar o hacer respetar las obligaciones contempladas en el Derecho de la Unión en materia de protección de los derechos fundamentales, en particular el derecho a la no discriminación, con respecto al uso de sistemas de IA de alto riesgo mencionados en el anexo III tendrán la facultad de solicitar y acceder a cualquier documentación creada o conservada con arreglo al presente Reglamento cuando el acceso a dicha documentación sea necesario para el ejercicio de las competencias derivadas de sus mandatos, dentro de los límites de su jurisdicción. La autoridad o el organismo público pertinente informará sobre dicha solicitud a la autoridad de vigilancia del mercado del Estado miembro que corresponda.

4. A más tardar 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 3 y las enumerará en la lista pública disponible. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

5. Cuando la documentación mencionada en el apartado 3 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión destinadas a proteger los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 3 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable tras la presentación de la solicitud.

6. Cualquier información y documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 3 con arreglo a las disposiciones recogidas en el presente artículo se tratarán de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 70.

Artículo 65

Procedimiento aplicable a los sistemas de IA que presenten un riesgo a nivel nacional

1. Los sistemas de IA que presenten un riesgo se entenderán como productos que presentan un riesgo según la definición del artículo 3, punto 19, del Reglamento (UE) 2019/1020 en lo que respecta a los riesgos para la salud, la seguridad o los derechos fundamentales de las personas.

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 según lo contemplado en el apartado 1, efectuará una evaluación del sistema de IA de que se trate para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Cuando se identifiquen riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 64, apartado 3. Los operadores pertinentes cooperarán en lo necesario con las autoridades de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 64, apartado 3.

   Cuando, en el curso de tal evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad determine.

   La autoridad de vigilancia del mercado informará al organismo notificado correspondiente en consecuencia. El artículo 18 del Reglamento (UE) 2019/1020 será de aplicación a las medidas mencionadas en el párrafo segundo.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya instado al operador a adoptar.

4. El operador se asegurará de que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en toda la Unión.

5. Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA en su mercado nacional, retirarlo de dicho mercado o recuperarlo. Dicha autoridad notificará estas medidas sin demora indebida a la Comisión y a los demás Estados miembros.

6. La notificación mencionada en 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, la naturaleza de la presunta no conformidad y del riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos formulados por el operador de que se trate. En particular, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno o varios de los motivos siguientes:

-a) incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5;

a) el incumplimiento de los requisitos establecidos en el título III, capítulo 2, por parte del sistema de IA de alto riesgo;

b) deficiencias en las normas armonizadas o especificaciones comunes mencionadas en los artículos 40 y 41 que confieren la presunción de conformidad.

c) el incumplimiento de las disposiciones establecidas en el artículo 52;

d) el incumplimiento por parte de los sistemas de IA de uso general de los requisitos y obligaciones a que se refiere el artículo 4 *bis*;

7. Las autoridades de vigilancia del mercado de los Estados miembros distintas de la autoridad de vigilancia del mercado del Estado miembro que inició el procedimiento comunicarán sin demora indebida a la Comisión y a los demás Estados miembros toda medida que adopten y cualquier información adicional de que dispongan sobre la no conformidad del sistema de IA en cuestión y, en caso de desacuerdo con la medida nacional notificada, sus objeciones al respecto.

8. Si, en el plazo de tres meses desde la recepción de la notificación indicada en el apartado 5, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por un Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador correspondiente con arreglo al artículo 18 del Reglamento (UE) 2019/1020. El plazo a que se refiere la primera frase del presente apartado se reducirá a treinta días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5.

9. Las autoridades de vigilancia del mercado de todos los Estados miembros velarán entonces por que se adopten sin demora indebida las medidas restrictivas adecuadas respecto del sistema de IA de que se trate, tales como la retirada del producto del mercado.

Artículo 66

Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación indicada en el artículo 65, apartado 5, o de treinta días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5, un Estado miembro formule objeciones sobre una medida adoptada por otro Estado miembro, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora indebida con la autoridad de vigilancia del mercado y el operador u operadores pertinentes del Estado miembro , y evaluará la medida nacional. Sobre la base de los resultados de la mencionada evaluación, la Comisión adoptará, en un plazo de nueve meses o de sesenta días en caso de incumplimiento de la prohibición de las prácticas de inteligencia artificial a que se refiere el artículo 5, a partir de la notificación a que se refiere el artículo 65, apartado 5, una decisión en la que indicará si la medida nacional está justificada o no. Deberá notificar dicha decisión al Estado miembro correspondiente. La Comisión también informará a todos los demás Estados miembros de tal decisión.

2. Si la Comisión considera justificada la medida adoptada por la autoridad de vigilancia del mercado del Estado miembro pertinente, las autoridades de vigilancia del mercado de todos los Estados miembros velarán por que se adopten las medidas restrictivas adecuadas con respecto al sistema de IA en cuestión, como la retirada del sistema de IA de su mercado sin demora indebida, e informarán de ello a la Comisión. Si la Comisión considera que la medida nacional no está justificada, la autoridad de vigilancia del mercado del Estado miembro de que se trate retirará la medida e informará de ello a la Comisión.

3. Cuando se considere que la medida nacional está justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a las que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n.º 1025/2012.

Artículo 67

Sistemas de IA de alto riesgo o de uso general conformes que presenten un riesgo

1. Cuando, tras efectuar una evaluación con arreglo al artículo 65, la autoridad de vigilancia del mercado de un Estado miembro compruebe que un sistema de IA de alto riesgo o de uso general, aunque conforme con arreglo al presente Reglamento, presenta un riesgo para la salud o la seguridad de las personas o para los derechos fundamentales, pedirá al operador correspondiente que adopte todas las medidas adecuadas para asegurarse de que el sistema de IA de que se trate ya no presente ese riesgo cuando se introduzca en el mercado o se ponga en servicio, o bien para retirarlo del mercado o recuperarlo sin demora indebida, dentro de un plazo que dicha autoridad determine.

2. El proveedor u otros operadores pertinentes se asegurarán de que se adoptan las medidas correctoras con respecto a todos los sistemas de IA afectados que hayan comercializado en toda la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. El Estado miembro informará inmediatamente a la Comisión y a los demás Estados miembros al respecto. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para identificar los sistemas de IA afectados y para determinar su origen, la cadena de suministro del sistema, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión consultará sin demora indebida a los Estados miembros afectados y al operador correspondiente y evaluará las medidas nacionales adoptadas. Sobre la base de los resultados de la evaluación, la Comisión adoptará una decisión en la que indicará si la medida está justificada o no y, en su caso, propondrá medidas adecuadas.

5. La Comisión enviará su decisión a los Estados miembros afectados e informará a todos los demás Estados miembros.

Artículo 68

Incumplimiento formal

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constate una de las situaciones indicadas a continuación, pedirá al proveedor correspondiente que subsane el incumplimiento de que se trate, dentro de un plazo que dicha autoridad determine:

   a) la colocación del marcado de conformidad no es conforme con el artículo 49;

   b) no se ha colocado el marcado de conformidad;

   c) no se ha elaborado la declaración UE de conformidad;

   d) la declaración UE de conformidad no se ha elaborado correctamente;

   e) no se ha colocado, en su caso, el número de identificación del organismo notificado que interviene en el procedimiento de evaluación de la conformidad.

2. Si el incumplimiento indicado en el apartado 1 persiste, el Estado miembro correspondiente adoptará todas las medidas adecuadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o garantizar que se recupera o se retira del mercado.

Artículo 68 bis

Instalaciones de ensayo de la Unión en el ámbito de la inteligencia artificial

1. La Comisión designará una o varias instalaciones de ensayo de la Unión de conformidad con el artículo 21 del Reglamento (UE) n.º 2019/1020 en el ámbito de la inteligencia artificial.

2. Sin perjuicio de las actividades de las instalaciones de ensayo de la Unión a que se refiere el artículo 21, apartado 6, del Reglamento (UE) n.º 2019/1020, las instalaciones de ensayo de la Unión a que se refiere el apartado 1 también proporcionarán asesoramiento técnico o científico independiente a petición del Comité o de las autoridades de vigilancia del mercado.

Artículo 68b

Grupo central de expertos independientes

1. A petición del Comité de IA, la Comisión adoptará, mediante un acto de ejecución, disposiciones sobre la creación, el mantenimiento y la financiación de un grupo central de expertos independientes para apoyar las actividades de aplicación en virtud del presente Reglamento.

2. Los expertos serán seleccionados por la Comisión e incluidos en el grupo central sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la inteligencia artificial, teniendo debidamente en cuenta los ámbitos técnicos cubiertos por los requisitos y obligaciones del presente Reglamento y las actividades de las autoridades de vigilancia del mercado con arreglo al artículo 11 del Reglamento (UE) n.º 2019/1020. La Comisión determinará el número de expertos que deben formar parte del grupo en función de las necesidades.

3. Los expertos podrán desempeñar las siguientes tareas:

a) asesorar y apoyar la labor de las autoridades de vigilancia del mercado, a petición de estas;

b) apoyar las investigaciones transfronterizas de vigilancia del mercado a que se refiere el artículo 58, letra h), sin perjuicio de las competencias de las autoridades de vigilancia del mercado;

c) asesorar y apoyar a la Comisión en el desempeño de sus funciones en el contexto de la cláusula de salvaguardia con arreglo al artículo 66.

4. Los expertos desempeñarán sus funciones con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el desempeño de sus tareas y actividades. Cada experto cumplimentará una declaración de intereses que se hará pública. La Comisión establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

5. Se podrá exigir a los Estados miembros que paguen tasas por el asesoramiento y el apoyo de los expertos. La estructura y el nivel de las tasas, así como el baremo y la estructura de los costes recuperables, serán adoptados por la Comisión mediante el acto de ejecución a que se refiere el apartado 1, teniendo en cuenta los objetivos de una aplicación adecuada del presente Reglamento, la rentabilidad y la necesidad de garantizar un acceso efectivo a los expertos por parte de todos los Estados miembros.

6. La Comisión facilitará el acceso oportuno de los Estados miembros a los expertos, según sea necesario, y garantizará que la combinación de actividades de apoyo llevadas a cabo por las instalaciones de ensayo de la Unión con arreglo al artículo 68 *bis* y los expertos con arreglo al presente artículo se organice de manera eficiente y aporte el mejor valor añadido posible.

TÍTULO IX

CÓDIGOS DE CONDUCTA

Artículo 69

Códigos de conducta para la aplicación voluntaria de requisitos específicos

1. La Comisión y los Estados miembros facilitarán la elaboración de códigos de conducta destinados a fomentar la aplicación voluntaria de uno o varios de los requisitos establecidos en el título III, capítulo 2, del presente Reglamento a sistemas de IA distintos de los de alto riesgo en la mayor medida posible, teniendo en cuenta las soluciones técnicas disponibles que permitan la aplicación de dichos requisitos.

2. La Comisión y los Estados miembros facilitarán la elaboración de códigos de conducta destinados a fomentar la aplicación voluntaria a todos los sistemas de IA de los requisitos específicos relativos, por ejemplo, a la sostenibilidad ambiental, en particular la programación eficiente desde el punto de vista energético, la accesibilidad para personas con discapacidad, la participación de las partes interesadas en el diseño y desarrollo de los sistemas de IA y la diversidad de los equipos de desarrollo, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos. La Comisión y los Estados miembros también facilitarán, cuando proceda, la elaboración de códigos de conducta aplicables con carácter voluntario relativos a las obligaciones de los usuarios en relación con los sistemas de IA.

3. Los códigos de conducta aplicables con carácter voluntario podrán ser elaborados por proveedores individuales de sistemas de IA, por organizaciones que los representen o por ambos, también con la participación de usuarios y de cualquier parte interesada y sus organizaciones representativas, o, cuando corresponda, por usuarios en lo que respecta a sus obligaciones. Los códigos de conducta podrán abarcar uno o varios sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes.

4. La Comisión y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de los proveedores que sean pymes, en particular empresas emergentes, cuando fomenten y faciliten la elaboración de los códigos de conducta a que se refiere el presente artículo.

TÍTULO X

CONFIDENCIALIDAD Y SANCIONES

Artículo 70
Confidencialidad

1. Las autoridades nacionales competentes, los organismos notificados, la Comisión, el Comité y cualquier otra persona física o jurídica involucrada en la aplicación del presente Reglamento adoptarán, de conformidad con el Derecho de la Unión o nacional, las medidas técnicas y organizativas adecuadas para garantizar la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, 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 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas;

b) la aplicación eficaz del presente Reglamento, en particular a efectos de investigaciones, inspecciones o auditorías;

c) los intereses públicos y de seguridad nacional;

d) la integridad de las causas penales o los procedimientos administrativos;

e) la integridad de la información clasificada de conformidad con el Derecho de la Unión o nacional.

2. Sin perjuicio de lo dispuesto en el apartado 1, la información intercambiada de forma confidencial entre las autoridades nacionales competentes y entre estas y la Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al usuario cuando las autoridades encargadas de la aplicación de la ley, del control de fronteras o las autoridades de inmigración o de asilo utilicen los sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III y dicha divulgación pudiera comprometer los intereses públicos y de seguridad nacional. Esta obligación de intercambio de información no incluirá los datos operativos delicados relativos a las actividades de las autoridades encargadas de la aplicación de la ley, el control de fronteras, la inmigración o el asilo.

Cuando las autoridades encargadas de la aplicación de la ley o las autoridades de inmigración o de asilo sean proveedores de sistemas de IA de alto riesgo a que se refieren los puntos 1, 6 y 7 del anexo III, la documentación técnica mencionada en el anexo IV permanecerá dentro de las instalaciones de dichas autoridades. Dichas autoridades velarán por que las autoridades de vigilancia del mercado a que se refiere el artículo 63, apartados 5 y 6, según proceda, puedan, previa solicitud, acceder inmediatamente a la documentación u obtener una copia de esta. Tan solo se permitirá acceder a dicha documentación o a cualquier copia de esta al personal de la autoridad de vigilancia del mercado que disponga de un nivel adecuado de habilitación de seguridad.

3. Los apartados 1 y 2 no afectarán a los derechos y obligaciones de la Comisión, los Estados miembros y sus autoridades pertinentes, ni de los organismos notificados en lo que se refiere al intercambio de información y la difusión de advertencias, en particular en el contexto de la cooperación transfronteriza, ni a las obligaciones de facilitar información que incumban a las partes interesadas en virtud del Derecho penal de los Estados miembros.

Artículo 71
Sanciones

1. De conformidad con los términos y condiciones establecidos en el presente Reglamento, los Estados miembros determinarán el régimen de sanciones, incluidas las multas administrativas, aplicable a las infracciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación adecuada y efectiva. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias. Tendrán particularmente en cuenta el tamaño y los intereses de los proveedores que sean pymes, en particular las empresas emergentes, así como su viabilidad económica. También tendrán en cuenta si el uso del sistema de IA se realiza en el contexto de una actividad personal no profesional.

2. Los Estados miembros comunicarán sin demora a la Comisión el régimen establecido y las medidas adoptadas, así como cualquier modificación posterior de los mismos.

3. El incumplimiento de cualquiera de las prohibiciones de las prácticas de inteligencia artificial a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 30 000 000 EUR o, si el infractor es una empresa, de hasta el 6 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior. En el caso de las pymes, en particular las empresas emergentes, estas multas ascenderán hasta el 3 % de su volumen de negocios anual mundial durante el ejercicio financiero anterior.

4. El incumplimiento de las siguientes disposiciones relacionadas con los operadores o los organismos notificados estará sujeto a multas administrativas de hasta 20 000 000 EUR o, si el infractor es una empresa, de hasta el 4 % de su volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior:

-a) las obligaciones de los proveedores con arreglo a los artículos 4 *ter* y 4 *quater*;

a) las obligaciones de los proveedores con arreglo al artículo 16;

b) las obligaciones de otras personas con arreglo al artículo 23 *bis*;

c) las obligaciones de los representantes autorizados con arreglo al artículo 25;

d) las obligaciones de los importadores con arreglo al artículo 26;

e) las obligaciones de los distribuidores con arreglo al artículo 27;

f) las obligaciones de los usuarios con arreglo al artículo 29, apartados 1 a 6 *bis*;

g) requisitos y obligaciones de los organismos notificados con arreglo al artículo 33, artículo 34, apartados 1, 3 y 4, y artículo 34 *bis*;

h) obligaciones de transparencia para los proveedores y usuarios con arreglo al artículo 52.

En el caso de las pymes, en particular las empresas emergentes, estas multas ascenderán hasta el 2 % de su volumen de negocios anual mundial durante el ejercicio financiero anterior.

5. La presentación de información inexacta, incompleta o engañosa a organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 10 000 000 EUR o, si el infractor es una empresa, de hasta el 2 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior. En el caso de las pymes, en particular las empresas emergentes, estas multas ascenderán hasta el 1 % de su volumen de negocios anual mundial durante el ejercicio financiero anterior.

6. Al decidir la cuantía de la multa administrativa en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación correspondiente y se tendrá debidamente en cuenta lo siguiente:

a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

a *bis*) la intencionalidad o negligencia en la infracción;

a *ter*) cualquier medida adoptada por el operador para poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

b) si otras autoridades de vigilancia del mercado de otros Estados miembros han impuesto ya multas administrativas al mismo operador por la misma infracción;

b *bis*) si otras autoridades ya han impuesto multas administrativas al mismo operador por infracciones de otra legislación nacional o de la Unión, cuando dichas infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;

c) el tamaño, el volumen de negocio anual y la cuota de mercado del operador que comete la infracción;

d) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

7. Cada Estado miembro establecerá normas que determinen si es posible, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que las multas las impongan órganos jurisdiccionales nacionales competentes u otros organismos, según proceda en dichos Estados miembros. La aplicación de dichas normas en estos Estados miembros tendrá un efecto equivalente.

9. El ejercicio por una autoridad de vigilancia del mercado de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

Artículo 72

Multas administrativas a instituciones, agencias y organismos de la Unión

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, las agencias y los organismos de la Unión comprendidos en el ámbito de aplicación del presente Reglamento. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y se tendrá debidamente en cuenta lo siguiente:

   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

   b) la cooperación con el Supervisor Europeo de Protección de Datos con el fin de poner remedio a la infracción y mitigar sus posibles efectos adversos, incluido el cumplimiento de cualquiera de las medidas que el propio Supervisor Europeo de Protección de Datos haya ordenado previamente contra la institución, agencia u organismo de la Unión de que se trate en relación con el mismo asunto;

   c) toda infracción anterior similar cometida por la institución, agencia u organismo de la Unión.

2. El incumplimiento de cualquiera de las prohibiciones de las prácticas de inteligencia artificial a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 500 000 EUR.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento distintos de los dispuestos en los artículos 5 y 10 será objeto de multas administrativas de hasta 250 000 EUR.

4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, agencia u organismo de la Unión sometida al procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída en lo que respecta a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en los elementos y las circunstancias sobre las que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, estarán estrechamente vinculadas al procedimiento.

5. Los derechos de defensa de las partes estarán garantizados plenamente en el curso del procedimiento. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas físicas y las empresas en la protección de sus datos personales o secretos comerciales.

6. La recaudación proveniente de la imposición de multas con arreglo al presente artículo pasará a engrosar los ingresos del presupuesto general de la Unión.

TÍTULO XI

DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

Artículo 73
Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. La delegación de poderes a que se refieren el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, y el artículo 48, apartado 5, se otorgará a la Comisión por un periodo de cinco años a partir de [*la fecha de entrada en vigor del 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 el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, y el artículo 48, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de poderes especificada en dicha decisión. La decisión surtirá efecto al día siguiente 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. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, y el artículo 48, apartado 5, entrarán en vigor únicamente 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. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 74
Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

TÍTULO XII

DISPOSICIONES FINALES

Artículo 75
Modificación del Reglamento (CE) n.º 300/2008

En el artículo 4, apartado 3, del Reglamento (CE) n.º 300/2008, se añade el párrafo siguiente:

«Al adoptar medidas detalladas relativas a las especificaciones técnicas y los procedimientos de aprobación y utilización del equipo de seguridad en relación con sistemas de inteligencia artificial en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 76

Modificación del Reglamento (UE) n.º 167/2013

En el artículo 17, apartado 5, del Reglamento (UE) n.º 167/2013, 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) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 77

Modificación del Reglamento (UE) n.º 168/2013

En el artículo 22, apartado 5, del Reglamento (UE) n.º 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) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 78

Modificación de la Directiva 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

«4. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, la Comisión tendrá en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento al desempeñar sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 79

Modificación de la Directiva (UE) 2016/797

En el artículo 5 de la Directiva (UE) 2016/797, se añade el apartado siguiente:

«12. Al adoptar actos delegados en virtud del apartado 1 y actos de ejecución en virtud del apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 80

Modificación del Reglamento (UE) 2018/858

En el artículo 5 del Reglamento (UE) 2018/858, se añade el apartado siguiente:

«4. Al adoptar actos delegados en virtud del apartado 3 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 81

Modificación del Reglamento (UE) 2018/1139

El Reglamento (UE) 2018/1139 se modifica como sigue:

1) En el artículo 17, se añade el apartado siguiente:

«3. Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [*relativo a la inteligencia artificial*] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

2) En el artículo 19, se añade el apartado 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) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

3) En el artículo 43, se añade el apartado siguiente:

«4. Al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

4) En el artículo 47, se añade el apartado siguiente:

«3. 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) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

5) En el artículo 57, se añade el apartado siguiente:

«Al adoptar dichos actos de ejecución en relación con sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

6) En el artículo 58, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial], se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.».

Artículo 82
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 en virtud del apartado 2 en relación con sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] del Parlamento Europeo y del Consejo*, se tendrán en cuenta los requisitos establecidos en el título III, capítulo 2, de dicho Reglamento.

_____

* Reglamento (UE) AAAA/XX [relativo a la inteligencia artificial] (DO …).».

Artículo 83

Sistemas de IA ya introducidos en el mercado o puestos en servicio

1. El presente Reglamento no se aplicará a los sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo IX que hayan sido introducidos en el mercado o puestos en servicio antes de *[12 meses después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2]*, salvo que la sustitución o modificación de dichos actos legislativos redunde en un cambio significativo en el diseño o la finalidad prevista del sistema o sistemas de IA de que se trate.

   Los requisitos establecidos en el presente Reglamento se tendrán en cuenta, en su caso, en la evaluación de cada sistema informático de gran magnitud establecido por los actos legislativos enumerados en el anexo IX que se efectúe de conformidad con dichos actos respectivos.

2. El presente Reglamento se aplicará a los sistemas de IA de alto riesgo distintos de los contemplados en el apartado 1 que hayan sido introducidos en el mercado o puestos en servicio antes de [*fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2*] únicamente si, a partir de dicha fecha, los sistemas mencionados se ven sometidos a cambios significativos en su diseño o su finalidad prevista.

Artículo 84

Evaluación y revisión

1. [suprimido]

1 *ter*) La Comisión evaluará la necesidad de modificar la lista del anexo III cada veinticuatro meses a partir de la entrada en vigor del presente Reglamento y hasta el final del periodo de delegación de poderes. Las conclusiones de dicha evaluación se presentarán al Parlamento Europeo y al Consejo.

2. A más tardar [*tres años después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2*] y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

3. Los informes mencionados en el apartado 2 prestarán una atención especial a lo siguiente:

   a) el estado de los recursos financieros, los equipos técnicos y los recursos humanos de las autoridades nacionales competentes para desempeñar de forma eficaz las funciones asignadas en virtud del presente Reglamento;

   b) el estado de las sanciones y, en particular, de las multas administrativas a que se refiere el artículo 71, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento.

4. En los [*tres años siguientes a la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2*] y posteriormente cada cuatro años, la Comisión evaluará el impacto y la eficacia de los códigos de conducta para promover la aplicación de los requisitos establecidos en el título III, capítulo 2, y en su caso otros requisitos adicionales, a los sistemas de IA distintos de los sistemas de IA de alto riesgo.

5. A efectos de lo dispuesto en los apartados 1 *bis* a 4, el Comité, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión a petición de esta.

6. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 *bis* a 4, la Comisión tendrá en cuenta las posiciones y conclusiones del Comité, el Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

7. La Comisión presentará, en caso necesario, las propuestas oportunas de modificación del presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología y a la vista de los avances en la sociedad de la información.

Artículo 85

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento se aplicará a partir de [treinta y seis meses tras la entrada en vigor del Reglamento].

3. Como excepción a lo dispuesto en el apartado 2:

   a) el título III, capítulo 4, y el título IV se aplicarán a partir de [doce meses tras la entrada en vigor del presente Reglamento];

   b) el artículo 71 se aplicará a partir de [doce meses tras la entrada en vigor del presente Reglamento].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta / El Presidente	*La Presidenta / El Presidente*

ANEXO I

[Eliminado]

ANEXO II

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 relativo a las 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 las embarcaciones de recreo y a las 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 en materia de 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, sobre la armonización de las legislaciones de los Estados miembros en materia de 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, relativa a la armonización de las legislaciones de los Estados miembros sobre 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, relativo a los 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 que queman combustibles gaseosos 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 los 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 por el que 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 los 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

1. Reglamento (CE) n.º 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) n.º 2320/2002 (DO L 97 de 9.4.2008, p. 72);

2. Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 52);

3. Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 1);

4. 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);

5. 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);

6. 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 sus remolques y de los sistemas, los componentes y las 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 por el que se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1);

7. Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los 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 de la Comisión (DO L 325 de 16.12.2019, p 1);

8. 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 la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010, (CE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y 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), en la medida en la que afecte al diseño, la producción y la comercialización de aeronaves contemplados en el artículo 2, apartado 1, letras a) y b), cuando se refiera a aeronaves no tripuladas y sus motores, hélices, componentes y equipos para controlarlas a distancia.

ANEXO III
SISTEMAS DE IA DE ALTO RIESGO A QUE SE REFIERE EL ARTÍCULO 6, APARTADO 3

En cada uno de los ámbitos enumerados en los puntos 1 a 8, los sistemas de IA mencionados específicamente en cada letra se consideran sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 3:

1. Biometría:

   a) sistemas de identificación biométrica remota.

2. Infraestructuras críticas:

   (a) sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y funcionamiento de infraestructuras digitales críticas, del tráfico rodado y del suministro de agua, gas, calefacción y electricidad.

3. Educación y formación profesional:

   (a) sistemas de IA destinados a utilizarse para determinar el acceso o la admisión de personas físicas a programas o centros educativos y de formación profesional a todos los niveles o para asignar a personas físicas a dichos programas o centros;

   (b) sistemas de IA destinados a utilizarse para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en programas o centros educativos y de formación profesional a todos los niveles.

4. Empleo, gestión de los trabajadores y acceso al autoempleo:

   (a) sistemas de IA destinados a utilizarse para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos;

(b) IA destinada a utilizarse para tomar decisiones relativas a la promoción y a la rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales y para realizar un seguimiento y una evaluación del rendimiento y el comportamiento de las personas en el marco de dichas relaciones.

5. Acceso a servicios privados esenciales y a servicios y ayudas públicos esenciales y disfrute de dichos servicios y ayudas:

(a) sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para acceder a servicios y ayudas esenciales de asistencia pública, así como para conceder, reducir, retirar o recuperar dichos servicios y ayudas;

(b) sistemas de IA destinados a utilizarse para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA puestos en servicio por proveedores que son microempresas y pequeñas empresas, tal como se definen en el anexo de la Recomendación 2003/361/CE de la Comisión, para su uso propio;

(c) sistemas de IA destinados a utilizarse para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo bomberos y servicios de asistencia médica;

(d) sistemas de IA destinados a utilizarse para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud, con excepción de los sistemas de IA puestos en servicio por proveedores que sean microempresas y pequeñas empresas, tal como se definen en el anexo de la Recomendación 2003/361/CE de la Comisión, para su propio uso.

6. Asuntos relacionados con la aplicación de la ley:

(a) sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley o en su nombre para evaluar el riesgo de que una persona física cometa una infracción o reincida o el riesgo de que una persona física se convierta en posible víctima de infracciones penales;

(b) sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley o en su nombre como polígrafos y herramientas similares, o para detectar el estado emocional de una persona física;

(c) [suprimido]

(d) sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley o en su nombre para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de infracciones penales;

(e) sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley o en su nombre para predecir la comisión o reiteración de una infracción penal real o potencial a partir de la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680, o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o grupos;

(f) sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley o en su nombre para elaborar perfiles de personas físicas, como se menciona en el artículo 3, punto 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de infracciones penales.

(g) [suprimido]

7. Gestión de la migración, el asilo y el control fronterizo:

(a) sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o en su nombre como polígrafos y herramientas similares, o para detectar el estado emocional de una persona física;

(b) sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o en su nombre para evaluar un riesgo, como un riesgo para la seguridad, la salud o relativo a la migración irregular, que plantee una persona física que tenga la intención de entrar o haya entrado en el territorio de un Estado miembro;

(c) [suprimido]

(d) sistemas de IA destinados a ser utilizados por las autoridades públicas competentes o en su nombre para examinar las solicitudes de asilo, visado y permiso de residencia, y las reclamaciones asociadas con respecto a la admisibilidad de las personas físicas solicitantes.

8. Administración de justicia y procesos democráticos:

(a) sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para interpretar hechos o la ley, así como para aplicar la ley a un conjunto concreto de hechos.

ANEXO IV
DOCUMENTACIÓN TÉCNICA A QUE SE REFIERE EL ARTÍCULO 11, APARTADO 1

La documentación técnica a que se refiere el artículo 11, apartado 1, incluirá como mínimo la siguiente información, aplicable al sistema de IA pertinente:

1. Una descripción general del sistema de IA que incluya:

   (a) su finalidad prevista, la persona o personas responsables de su desarrollo, la fecha y la versión del sistema;

   (b) cómo el sistema de IA interactúa o puede utilizarse para interactuar con los soportes físicos o el software que no formen parte del propio sistema de IA, cuando proceda;

   (c) las versiones de software y microprogramas pertinentes y todo requisito relacionado con la actualización de versiones;

   (d) la descripción de todas las formas en que el sistema de IA se ha introducido en el mercado o puesto en servicio (por ejemplo, en un paquete de *software* integrado en el *hardware*, mediante una descarga, una API, etc.);

   (e) la descripción del soporte físico en el que se prevé que opere el sistema de IA;

   (f) en caso de que el sistema de IA consista en un componente de productos, fotografías o ilustraciones de las características exteriores, el marcado y la configuración interna de dichos productos;

   (g) instrucciones de uso para el usuario y, cuando proceda, instrucciones de instalación.

2. Una descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, incluidos:

   (a) los métodos y las medidas adoptados para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas previamente entrenados facilitados por terceros y cómo se han utilizado, integrado o modificado por parte del proveedor;

(b) las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA y de los algoritmos; las opciones clave de diseño, en particular, la justificación lógica y las hipótesis planteadas, también con respecto a las personas o grupos de personas en relación con los que se prevé utilizar el sistema; las principales opciones de clasificación; aquello que el sistema está diseñado para optimizar y la pertinencia de los diversos parámetros; la descripción de los resultados esperados del sistema; las decisiones adoptadas acerca de cualquier posible efecto de compensación con respecto a las soluciones técnicas adoptadas para dar cumplimiento a los requisitos establecidos en el título III, capítulo 2;

(c) la descripción de la arquitectura del sistema que detalle cómo se incorporan o enriquecen mutuamente los componentes del software, y cómo se integran en el procesamiento general; los recursos informáticos utilizados para el desarrollo, el entrenamiento, la prueba y la validación del sistema de IA;

(d) cuando proceda, los requisitos sobre datos en forma de fichas técnicas que describan las metodologías y técnicas de entrenamiento, así como los conjuntos de datos de entrenamiento utilizados, e incluyan una descripción general de dichos conjuntos de datos e información acerca de su procedencia, su alcance y sus características principales; cómo se obtuvieron y seleccionaron los datos; los procedimientos de etiquetado (p. ej., para el aprendizaje supervisado), las metodologías de depuración de datos (p. ej., la detección de anomalías);

(e) la evaluación de las medidas de vigilancia humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios, con arreglo al artículo 13, apartado 3, letra d);

(f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su funcionamiento, junto con toda la información pertinente relativa a las soluciones técnicas adoptadas con el objetivo de garantizar que el sistema de IA cumpla de forma continua los requisitos pertinentes establecidos en el título III, capítulo 2;

(g) los procedimientos de validación y prueba utilizados, incluida la información acerca de los datos de validación y prueba empleados y sus características principales; los parámetros utilizados para medir la precisión, la solidez, la ciberseguridad y el cumplimiento de otros requisitos pertinentes dispuestos en el título III, capítulo 2, así como los efectos potencialmente discriminatorios; los archivos de registro de las pruebas y todos los informes de las pruebas fechados y firmados por las personas responsables, en particular en lo que respecta a los cambios predeterminados a que se refiere la letra f).

3. Información detallada acerca del seguimiento, el funcionamiento y el control del sistema de IA, en particular con respecto a: sus capacidades y limitaciones de funcionamiento, incluidos los niveles de precisión para las personas o grupos de personas específicos con respecto a los que se prevé utilizar el sistema y el nivel de precisión general esperado en relación con su finalidad prevista; los resultados no deseados previsibles y las fuentes de riesgo 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 vigilancia humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios; las especificaciones de los datos de entrada, según proceda.

4. Una descripción detallada del sistema de gestión de riesgos con arreglo al artículo 9.

5. Una descripción de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida.

6. 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 normas armonizadas, una descripción detallada de las soluciones adoptadas para cumplir los requisitos establecidos en el título III, capítulo 2, incluida una lista de otras normas y especificaciones técnicas pertinentes que se hayan aplicado.

7. Una copia de la declaración UE de conformidad.

8. Una descripción detallada del sistema establecido para evaluar el funcionamiento del sistema de IA en la fase posterior a la comercialización, de conformidad con el artículo 61, incluido el plan de vigilancia poscomercialización a que se refiere el artículo 61, apartado 3.

ANEXO V
DECLARACIÓN UE DE CONFORMIDAD

La declaración UE de conformidad a que se hace referencia en el artículo 48 contendrá toda la información siguiente:

1. El nombre y tipo del sistema de IA, y toda referencia inequívoca adicional que permita la identificación y trazabilidad del sistema de IA.

2. El nombre y dirección del proveedor y, en su caso, de su representante autorizado.

3. La afirmación de que la declaración UE de conformidad se emite bajo la exclusiva responsabilidad del proveedor.

4. La afirmación de que el sistema de IA en cuestión es conforme con el presente Reglamento y, en su caso, con cualquier otra legislación pertinente de la Unión que disponga la emisión de una declaración UE de conformidad.

5. Referencias a todas las normas armonizadas pertinentes utilizadas o a cualquier otra especificación común respecto a las cuales se declara la conformidad.

6. En su caso, el nombre y número de identificación del organismo notificado, una descripción del procedimiento de evaluación de la conformidad llevado a cabo y la identificación del certificado emitido.

7. El lugar y la fecha de emisión de la declaración, el nombre y el cargo de la persona que la firme, la indicación de en nombre o por cuenta de quién lo hace, y la firma.

ANEXO VI
PROCEDIMIENTO DE EVALUACIÓN DE LA CONFORMIDAD FUNDAMENTADO EN UN CONTROL INTERNO

1. El procedimiento de evaluación de la conformidad fundamentado en un 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 es conforme con los requisitos establecidos en el artículo 17.

3. El proveedor examina la información presente en la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en el título III, capítulo 2.

4. Asimismo, el proveedor verifica que el proceso de diseño y desarrollo del sistema de IA y su vigilancia poscomercialización a que se refiere el artículo 61 es coherente con la documentación técnica.

ANEXO VII
CONFORMIDAD BASADA EN LA EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA CALIDAD Y LA EVALUACIÓN DE LA DOCUMENTACIÓN TÉCNICA

1. Introducción

La conformidad basada en la evaluación del sistema de gestión de la calidad y la 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, el desarrollo y la prueba de los sistemas de IA en virtud del artículo 17 se examinará de conformidad con el punto 3 y estará sujeto a vigilancia con arreglo a lo establecido 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 incluirá:

(a) el nombre y dirección del proveedor y, si es el representante autorizado quien presenta la solicitud, también el nombre y dirección de este;

(b) la lista de los sistemas de IA a los que se aplica el mismo sistema de gestión de la calidad;

(c) la documentación técnica para cada sistema de IA al que se aplica 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 por escrito 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 especificados en el artículo 17.

La decisión se notificará al proveedor 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 proveedor continuará aplicando y manteniendo el sistema de gestión de la calidad aprobado de forma 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 IA a los que este se aplica.

El organismo notificado examinará los cambios propuestos y decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2 o si es necesario realizar una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación incluirá 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 a que se refiere el punto 3, el proveedor presentará una solicitud ante el organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que el proveedor pretenda introducir en el mercado o poner en servicio y al que se aplique el sistema de gestión de la calidad mencionado en el punto 3.

4.2. La solicitud incluirá:

(a) el nombre y dirección del proveedor;

(b) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;

(c) la documentación técnica contemplada en el anexo IV.

4.3. El organismo notificado examinará la documentación técnica. Cuando proceda y se limite a lo necesario para el desempeño de sus tareas, se concederá al organismo notificado pleno acceso a los conjuntos de datos de entrenamiento, validación y prueba utilizados, también, cuando proceda y con sujeción a salvaguardias de seguridad, a través de interfaces de programación de aplicaciones (API) u otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor facilite más evidencias o lleve a cabo pruebas adicionales para lograr una evaluación adecuada de la conformidad del sistema de IA con los requisitos establecidos en el título III, capítulo 2. Cuando el organismo notificado no quede satisfecho con las pruebas realizadas por el proveedor, efectuará directamente las pruebas adecuadas, según proceda.

4.5. Se concederá a los organismos notificados acceso al código fuente del sistema de IA previa solicitud motivada y solo si se cumplen las siguientes condiciones acumulativas:

a) el acceso al código fuente es necesario para evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el título III, capítulo 2, y

b) los procedimientos y verificaciones de prueba/auditoría basados en los datos y la documentación facilitados por el proveedor se han agotado o han resultado insuficientes.

4.6. La decisión 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 un sistema de IA cumpla los requisitos establecidos en el título III, capítulo 2, el organismo notificado expedirá un certificado UE de evaluación de la documentación técnica. Dicho certificado indicará el nombre y dirección del proveedor, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para identificar el sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente para poder evaluar la conformidad del sistema de IA y permitir el control del sistema de IA mientras esté en uso, cuando proceda.

En caso de que el sistema de IA no cumpla los requisitos establecidos en el título III, capítulo 2, el organismo notificado se negará a expedir el certificado UE de evaluación de la documentación técnica e informará de ello al solicitante, motivando detalladamente su negativa.

Cuando el sistema de IA no cumpla los requisitos relativos a los datos utilizados para su entrenamiento, será necesario llevar a cabo un nuevo entrenamiento del sistema antes de presentar una solicitud para una nueva evaluación de la conformidad. En este caso, la decisión de evaluación motivada del organismo notificado que deniegue la expedición del certificado UE de evaluación de la documentación técnica contendrá consideraciones específicas relativas a los datos de calidad utilizados para entrenar el sistema de IA, especialmente acerca de los motivos del incumplimiento.

4.7. Cualquier cambio del sistema de IA que pueda afectar al cumplimiento de los requisitos o a su finalidad prevista estará sujeto a la aprobación del organismo notificado que haya expedido el certificado UE de evaluación de la documentación técnica. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios previamente mencionados o de si tiene constancia de que existan tales cambios. El organismo notificado evaluará los cambios previstos y decidirá si estos requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden abordarse mediante un suplemento al certificado UE de evaluación de la documentación técnica. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si se aprueban los cambios, le expedirá un suplemento al certificado UE de evaluación de la documentación técnica.

5. Vigilancia del sistema de gestión de la calidad aprobado

5.1. La finalidad de la vigilancia efectuada por el organismo notificado a que se refiere el punto 3 es asegurarse de que el proveedor cumpla debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de evaluación, el proveedor otorgará acceso al organismo notificado a las instalaciones donde se esté llevando a cabo el diseño, el desarrollo o la prueba de los sistemas de IA. El proveedor, a su vez, compartirá con el organismo notificado toda la información necesaria.

5.3. El organismo notificado realizará periódicamente auditorías para asegurarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad, y le entregará un informe de la auditoría. En el marco de dichas auditorías, el organismo notificado podrá efectuar pruebas adicionales de los sistemas de IA para los que se haya expedido un certificado UE de evaluación de la documentación técnica.

ANEXO VIII
INFORMACIÓN QUE DEBE PRESENTARSE PARA EL REGISTRO DE OPERADORES Y SISTEMAS DE IA DE ALTO RIESGO CONFORME AL ARTÍCULO 51

Los proveedores, los representantes autorizados y los usuarios que sean autoridades, agencias u organismos públicos presentarán la información a que se refiere la parte I. Los proveedores o, en su caso, los representantes autorizados velarán por que la información sobre sus sistemas de IA de alto riesgo a que se refiere la parte II, puntos 1 a 11, esté completa, sea correcta y se mantenga actualizada. La información establecida en la parte II, punto 12, será generada automáticamente por la base de datos.

Parte I. Información relativa a los operadores (para el registro de los operadores)

-1. Tipo de operador (proveedor, representante autorizado o usuario).

1. El nombre, dirección y datos de contacto del proveedor.

2. Cuando sea otra persona la que presente la información en nombre del operador, el nombre, dirección y datos de contacto de dicha persona.

Parte II. Información relacionada con el sistema de IA de alto riesgo

1. El nombre, dirección y datos de contacto del proveedor.

2. El nombre, dirección y datos de contacto del representante autorizado, en su caso.

3. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.

4. La descripción de la finalidad prevista del sistema de IA.

5. La situación del sistema de IA (comercializado o puesto en servicio; ha dejado de comercializarse/estar en servicio, recuperado).

6. El tipo, el número y la fecha de caducidad del certificado expedido por el organismo notificado y nombre o número de identificación de dicho organismo notificado, cuando proceda.

7. Una copia escaneada del certificado a que se refiere el punto 6, cuando proceda.

8. Los Estados miembros donde el sistema de IA esté o se haya introducido en el mercado o puesto en servicio o esté disponible en la Unión.

9. Una copia de la declaración UE de conformidad contemplada en el artículo 48.

10. Las instrucciones de uso electrónicas.

11. Una URL para obtener información adicional (opcional).

12. El nombre, dirección y datos de contacto de los usuarios.

ANEXO VIII *bis*

INFORMACIÓN QUE DEBE PRESENTARSE PARA EL 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 54 *BIS*

Con respecto a las pruebas en condiciones reales que deben inscribirse en el registro de conformidad con el artículo 54 *bis*, se facilitará y mantendrá actualizada la información siguiente:

1. número de identificación único para toda la Unión de la prueba en condiciones reales;

2. nombre y datos de contacto del proveedor o posible proveedor y de los usuarios que participen en la prueba en condiciones reales;

3. una breve descripción del sistema de IA, su finalidad prevista y demás información necesaria para la identificación del sistema;

4. un resumen de las principales características del plan de la prueba en condiciones reales;

5. información sobre la suspensión o la terminación de la prueba en condiciones reales.

ANEXO IX

LEGISLACIÓN DE LA UNIÓN EN MATERIA DE 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 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 las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 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 Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 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) Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (CE) n.º 767/2008, el Reglamento (CE) n.º 810/2009, el Reglamento (UE) 2017/2226, el Reglamento (UE) 2016/399, el Reglamento XX/2018 [Reglamento sobre interoperabilidad] y la Decisión 2004/512/CE, y se deroga la Decisión 2008/633/JAI del Consejo - COM(2018) 302 final. Se actualizará una vez los colegisladores adopten el Reglamento (abril/mayo de 2021).

3. Eurodac

(a) Propuesta modificada de REGLAMENTO 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) XXX/XXX [Reglamento sobre la gestión del asilo y la migración] y del Reglamento (UE) XXX/XXX [Reglamento sobre el Marco de Reasentamiento], para la identificación de un nacional de un tercer país o un apátrida en situación irregular, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 - COM(2020) 614 final.

4. Sistema de Entradas y Salidas

(a) Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, 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 de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican 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 (SEIAV) y por el que 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 objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV) (DO L 236 de 19.9.2018, p. 72).

6. Sistema Europeo de Información de Antecedentes Penales de 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 para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información 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, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los 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, relativo al establecimiento de 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).