Reglamento de Inteligencia Artificial de la Unión Europea

2024/1689

Nota introductoria

A continuación, se publica el *Reglamento del Parlamento Europeo y del Consejo de la Unión Europea sobre inteligencia artificial* (en adelante IA), el mismo que fue anunciado el trece de junio de 2024, documento por el cual se lleva a cabo una sistematización y síntesis de aquellas normas referentes a la IA. Uno de los objetivos de este reglamento es el de uniformizar la legislación vigente sobre el tema de IA en el ámbito de la Unión Europea, el énfasis que se brinda en las explicaciones para su elaboración es la necesaria correspondencia con *los valores de la Unión* y que el uso de la IA debe estar siempre centrada en el ser humano, manteniendo las consideraciones a una óptima calidad de vida y respeto a los derechos señalados en la Carta de los Derechos Fundamentales de la Unión Europea.

Dentro de sus propuestas está la de brindar un soporte jurídico integral para la innovación, garantizar un libre mercado en todo lo relacionado a la IA, dando prioridad a la dinamización de la economía tomando en cuenta el impacto de la IA; y, en lo posible evitar regulaciones ineficientes. Se busca con este reglamento uniformizar también las obligaciones de los operadores y garantizar los derechos de todos los actores que se desenvuelven en el mercado de la Unión Europea, todo ello, sin desmedro de la protección de las bases de datos personales.

Para fines didácticos, podemos dividir al reglamento en tres partes; en la primera, se hallan los considerandos, conceptos, aclaraciones y el ámbito de aplicación tanto en formas y contenidos; la segunda parte, es el reglamento en sí mismo; y, la tercera parte, contiene las disposiciones finales donde se subsumen aquellas

normas relativas a la IA que andaban dispersas —ahora, todo sistematizado en el flamante reglamento sobre IA—. Finalmente, se señala los anexos que contienen las actividades legislativas de los países miembros de la unión europea vinculados al tema de inteligencia artificial. Todo ello puede consultarlo en el enlace: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

En el escenario del acceso masivo a las nuevas tecnologías, el desborde de las herramientas informáticas y todo el ecosistema digital donde la IA va tornándose en protagonista, ese escenario nos hace reflexionar respecto de la importancia de contar con un marco jurídico idóneo para el uso de la IA, la importancia de tener en orden los conceptos a utilizarse. En el presente numero de la revista se publica el texto del reglamento de IA de la Unión Europea para desde el ámbito de la comparación jurídica sea de utilidad —en lo que corresponda— para atender dicho fenómeno en nuestro sistema jurídico.

Dirección de Publicaciones

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo [De la unión europea]

de 13 de junio de 2024

Por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

[…]

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto

1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.

2. El presente Reglamento establece:

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

b) prohibiciones de determinadas prácticas de IA;

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

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

e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general;

f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;

g) medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

Artículo 2
Ámbito de aplicación

1. El presente Reglamento se aplicará a:

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

b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión;

c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen 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;

f) los representantes autorizados de los proveedores que no estén establecidos en la Unión;

g) las personas afectadas que estén ubicadas en la Unión.

2. A los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en la sección B del anexo I, únicamente se les aplicará el artículo 6, apartado 1, y los artículos 102 a 109 y el artículo 112. El artículo 57 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del presente Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión.

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

El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas 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 o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas.

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

6. El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.

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

8. El presente Reglamento no se aplicará a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión.

9. El presente Reglamento se entenderá sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos.

10. El presente Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.

11. El presente Reglamento no impedirá que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores ni que fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores.

12. El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.

Artículo 3
Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

2) «riesgo»: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio;

3) «proveedor»: una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;

4) «responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional;

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

6) «importador»: una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país;

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

8) «operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor;

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

10) «comercialización»: el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente;

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

12) «finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, 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, incluidos otros sistemas de IA, razonablemente previsible;

14) «componente de seguridad»: un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, 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 responsable del despliegue, 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 responsables del despliegue, a inutilizarlo o a 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) «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 supervisión;

20) «evaluación de la conformidad»: el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo;

21) «organismo de evaluación de la conformidad»: un organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección;

22) «organismo notificado»: un organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otros actos pertinentes de la legislación de armonización de la Unión;

23) «modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectado el cumplimiento por parte del sistema de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate;

24) «marcado CE»: un marcado con el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo III, sección 2, y con otros actos aplicables de la legislación de armonización de la Unión que prevén su colocación;

25) «sistema de vigilancia poscomercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger 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 armonizada tal como se define 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 para, entre otras cosas, evitar el subajuste o el sobreajuste;

31) «conjunto de datos de validación»: un conjunto de datos independiente o una parte del conjunto de datos de entrenamiento, obtenida mediante una división fija o variable;

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

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

34) «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;

35) «identificación biométrica»: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos;

36) «verificación biométrica»: la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente;

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

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

39) «sistema de reconocimiento de emociones»: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos;

40) «sistema de categorización biométrica»: un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas;

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

42) «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 sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas;

43) «sistema de identificación biométrica remota en diferido»: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real;

44) «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 deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad;

45) «autoridad garante del cumplimiento del Derecho»:

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

   b) cualquier otro organismo 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 delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

46) «garantía del cumplimiento del Derecho»: las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

47) «Oficina de IA»: la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión;

48) «autoridad nacional competente»: una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos;

49) «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias:

   a) el fallecimiento de una persona o un perjuicio grave para su salud;

   b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;

   c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;

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

50) «datos personales»: los datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

51) «datos no personales»: los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

52) «elaboración de perfiles»: la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679;

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

54) «plan del espacio controlado de pruebas»: un documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos para las actividades realizadas en el espacio controlado de pruebas;

55) «espacio controlado de pruebas para la IA»: un marco controlado establecido por una autoridad competente que ofrece a los proveedores y proveedores potenciales 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 del espacio controlado de pruebas y durante un tiempo limitado, bajo supervisión regulatoria;

56) «alfabetización en materia de IA»: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar;

57) «prueba en condiciones reales»: la prueba temporal de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente Reglamento; si se cumplen todas las condiciones establecidas en el artículo 57 o 60, no se considerará una introducción en el mercado o una puesta en servicio del sistema de IA en el sentido de lo dispuesto en el presente Reglamento;

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

59) «consentimiento informado»: la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar;

60) «ultrasuplantación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos;

61) «infracción generalizada»: todo acto u omisión contrario al Derecho de la Unión por el que se protegen los intereses de las personas y que:

    a) haya perjudicado o pueda perjudicar los intereses colectivos de personas que residen en al menos dos Estados miembros distintos de aquel en el que:

        i) se originó o tuvo lugar el acto u omisión,

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

iii) esté establecido el responsable del despliegue en el momento de cometer la infracción;

b) haya perjudicado, perjudique o pueda perjudicar los intereses colectivos de las personas y tenga características comunes —incluidas la misma práctica ilícita o la vulneración del mismo interés— y sea cometido simultáneamente por el mismo operador en al menos tres Estados miembros;

62) «infraestructura crítica»: una infraestructura crítica tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2022/2557;

63) «modelo de IA de uso general»: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado;

64) «capacidades de gran impacto»: capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados;

65) «riesgo sistémico»: un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor;

66) «sistema de IA de uso general»: un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

67) «operación de coma flotante»: cualquier operación o tarea matemática que implique números de coma flotante, que son un subconjunto de los números reales normalmente representados en los ordenadores mediante un número entero de precisión fija elevado por el exponente entero de una base fija;

68) «proveedor posterior»: un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales.

Artículo 4
Alfabetización en materia de IA

Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un

nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas.

CAPÍTULO II
PRÁCTICAS DE IA PROHIBIDAS

Artículo 5
Prácticas de IA prohibidas

1. Quedan prohibidas las siguientes prácticas de IA:

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 o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas 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 colectivos de personas 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 colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose

únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, 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 víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

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

   iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de

los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y 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;

b) las consecuencias que tendría el uso del sistema en 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 garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

3. A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el

apartado 2. Dicha autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. 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 garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales 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 presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

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

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión.

CAPÍTULO III
SISTEMAS DE IA DE ALTO RIESGO

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

Artículo 6
Reglas de clasificación de los sistemas de IA de alto riesgo

1. Con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:

a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y

b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.

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

3. No obstante lo dispuesto en el apartado 2, un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones.

El párrafo primero se aplicará cuando se cumpla cualquiera de las condiciones siguientes:

a) que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;

b) que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;

c) que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o

d) que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

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

5. La Comisión, previa consulta al Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»), y a más tardar el 2 de febrero de 2026, proporcionará directrices que especifiquen la aplicación práctica del presente artículo en consonancia con el artículo 96, junto con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, añadiendo nuevas condiciones a las establecidas en dicho apartado, o modificando estas, cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas.

7. La Comisión adoptará actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, suprimiendo cualquiera de las condiciones establecidas en él, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento.

8. Ninguna modificación de las condiciones establecidas en el apartado 3, párrafo segundo, adoptada de conformidad con los apartados 6 y 7 del presente artículo, reducirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento, y cualquier modificación garantizará la coherencia con los actos delegados adoptados con arreglo al artículo 7, apartado 1, y tendrá en cuenta la evolución tecnológica y del mercado.

Artículo 7
Modificaciones del anexo III

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo III mediante la adición o modificación de casos de uso de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA estén destinados a ser utilizados en cualquiera de los ámbitos que figuran en el anexo III, y

b) que los sistemas de IA planteen un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales, y que dicho riesgo sea equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que plantean los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando evalúe la condición prevista en el apartado 1, letra b), 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 naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

d) el grado de autonomía con el que actúa el sistema de IA y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio;

e) 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 en los derechos fundamentales o haya dado lugar a problemas importantes en relación con la probabilidad de dicho perjuicio o dichas repercusiones negativas, según demuestren, por ejemplo, los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes o cualquier otro informe, según proceda;

f) 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 varias personas o afectar de manera desproporcionada a un determinado colectivo de personas;

g) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan del resultado generado por un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicho resultado;

h) la medida en que exista un desequilibrio de poder o las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del responsable del despliegue de un sistema de IA, en particular debido a su situación, autoridad, conocimientos, circunstancias económicas o sociales, o edad;

i) la medida en que sea fácil corregir o revertir el resultado generado utilizando un sistema de IA, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo y sin que deba considerarse que los resultados que afectan negativamente a la salud, la seguridad o los derechos fundamentales son fáciles de corregir o revertir;

j) la probabilidad de que el despliegue del sistema de IA resulte beneficioso para las personas, los colectivos o la sociedad en general, y la magnitud de este beneficio, incluidas posibles mejoras en la seguridad de los productos;

k) la medida en que el Derecho de la Unión vigente establezca:

i) vías de recurso efectivas en relación con los riesgos que plantea un sistema de IA, con exclusión de las acciones por daños y perjuicios,

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

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 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) que los sistemas de IA de alto riesgo de que se trate ya no planteen riesgos considerables para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

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

SECCIÓN 2
Requisitos de los sistemas de IA de alto riesgo

Artículo 8
Cumplimiento de los requisitos

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

2. Cuando un producto contenga un sistema de IA al que se apliquen los requisitos del presente Reglamento, así como los requisitos de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, los proveedores serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables en virtud de los actos legislativos de armonización de la Unión que sean aplicables. Para garantizar el cumplimiento de los sistemas de IA de alto riesgo a que se refiere el apartado 1 de los requisitos establecidos en la presente sección, y con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los procesos de prueba y presentación de información necesarios, y la información y la documentación que faciliten con respecto a su producto en documentación y procedimientos que ya existan y exijan los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A.

Artículo 9
Sistema de gestión de riesgos

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

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

a) la determinación y el análisis de los riesgos conocidos y previsibles que el sistema de IA de alto riesgo pueda plantear para la salud, la seguridad o los derechos fun-

damentales cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista;

b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

c) la evaluación de otros riesgos que podrían surgir, a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización a que se refiere el artículo 72;

d) la adopción de medidas adecuadas y específicas de gestión de riesgos diseñadas para hacer frente a los riesgos detectados con arreglo a la letra a).

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

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible interacción derivados de la aplicación combinada de los requisitos establecidos en la presente sección, con vistas a reducir al mínimo los riesgos de manera más eficaz al tiempo que se logra un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

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

A la hora de determinar 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 técnicamente viable 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 que hagan frente a los riesgos que no puedan eliminarse;

c) proporcionar la información requerida conforme al artículo 13 y, cuando proceda, impartir formación a los responsables del despliegue.

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

6. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de manera coherente con su finalidad prevista y cumplen los requisitos establecidos en la presente sección.

7. Los procedimientos de prueba podrán incluir pruebas en condiciones reales de conformidad con el artículo 60.

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

9. Cuando se implante el sistema de gestión de riesgos previsto en los apartados 1 a 7, los proveedores prestarán atención a si, en vista de su finalidad prevista, es probable que el sistema de IA de alto riesgo afecte negativamente a las personas menores de dieciocho años y, en su caso, a otros colectivos vulnerables.

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

Artículo 10
Datos y gobernanza de datos

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

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente:

a) las decisiones pertinentes relativas al diseño;

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

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

d) la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;

e) una evaluación 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, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;

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

h) la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y estarán completos en vista de su finalidad prevista. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los colectivos de personas en relación con los cuales está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos.

4. Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo.

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

a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización;

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

d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;

e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior;

f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones

por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

6. Para el desarrollo de sistemas de IA de alto riesgo que no empleen técnicas que impliquen el entrenamiento de modelos de IA, 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 elaborará 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 la presente sección y que proporcione de manera clara y completa a las autoridades nacionales competentes y a los organismos notificados la información necesaria para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV. Las pymes, incluidas las empresas emergentes, podrán facilitar los elementos de la documentación técnica especificada en el anexo IV de manera simplificada. A tal fin, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pequeñas empresas y las microempresas. Cuando una pyme, incluidas las empresas emergentes, opte por facilitar la información exigida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión mencionados en el anexo I, sección A, se elaborará un único conjunto de documentos técnicos que contenga toda la información mencionada en el apartado 1, así como la información que exijan dichos actos legislativos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 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 la presente sección.

Artículo 12
Conservación de registros

1. Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de acontecimientos (en lo sucesivo, «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 de alto riesgo que resulte adecuado para la finalidad prevista del sistema, las capacidades de registro permitirán que se registren acontecimientos pertinentes para:

a) la detección de situaciones que puedan dar lugar a que el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, o a una modificación sustancial;

b) la facilitación de la vigilancia poscomercialización a que se refiere el artículo 72, y

c) la vigilancia del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 26, apartado 5.

3. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), 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 responsables del despliegue

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.

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 responsables del despliegue.

3. Las instrucciones de uso contendrán al menos la siguiente información:

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

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

i) su finalidad prevista,

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 cualquier circunstancia conocida y previsible que pueda 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 o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere el artículo 9, apartado 2,

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

v) cuando proceda, su funcionamiento con respecto a determinadas personas o determinados colectivos de personas en relación con los que esté previsto utilizar el sistema,

vi) 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 de alto riesgo,

vii) en su caso, información que permita a los responsables del despliegue interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente;

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 supervisión humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue;

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

f) cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el artículo 12.

Artículo 14
Supervisión 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 herramientas de interfaz humano-máquina adecuadas.

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

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

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 responsable del despliegue.

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1, 2 y 3, el sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada a:

a) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;

b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;

c) interpretar correctamente los resultados 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 descartar, invalidar o revertir los resultados de salida que este genere;

e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

5. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación.

El requisito de la verificación por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando 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 alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.

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

3. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión de dichos sistemas, así como los parámetros pertinentes para medirla.

4. Los sistemas de IA de alto riesgo serán lo más resistentes posible en lo que respecta a los errores, fallos o incoherencias que pueden surgir en los propios sistemas o en el entorno en el que funcionan, en particular a causa de su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones 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 resultados de salida que pueden estar sesgados influyan en la información de entrada de futuras operaciones (bucles de retroalimentación) y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos adecuadas.

5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su 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, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento

(«envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo.

SECCIÓN 3

Obligaciones de los proveedores y responsables del despliegue 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 la sección 2;

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

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

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

e) 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 19;

f) 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;

g) elaborarán una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47;

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

i) cumplirán las obligaciones de registro a que se refiere el artículo 49, apartado 1;

j) adoptarán las medidas correctoras necesarias y facilitarán la información exigida en el artículo 20;

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

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

Artículo 17
Sistema de gestión de la calidad

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

a) una estrategia para el cumplimiento de la normativa, 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 del sistema de IA de alto riesgo y en el control y el aseguramiento de la calidad de este;

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 se ejecutarán;

e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes establecidos en la sección 2, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla dichos requisitos;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su adquisición, 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 esa finalidad;

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

h) el establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización de conformidad con el artículo 72;

i) los procedimientos asociados a la notificación de un incidente grave con arreglo al artículo 73;

j) la gestión de la comunicación con las autoridades nacionales competentes, otras autoridades pertinentes, incluidas las 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 para llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluidas medidas relacionadas con la seguridad del 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 aplicación de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor. Los proveedores respetarán, en todo caso, el grado de rigor y el nivel de protección requerido para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.

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

4. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho 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 en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

Artículo 18
Conservación de la documentación

1. Durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, 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 47.

2. 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 quiebre o cese en su actividad antes del final de dicho período.

3. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán la documentación técnica como parte de la documentación conservada en virtud del Derecho pertinente de la Unión en materia de servicios financieros.

Artículo 19
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 los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Sin perjuicio del Derecho aplicable de la Unión o nacional, los archivos de registro se conservarán durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que el Derecho de la Unión o nacional aplicable, en particular el Derecho de la Unión en materia de protección de datos personales, disponga otra cosa.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho 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 del Derecho pertinente en materia de servicios financieros.

Artículo 20
Medidas correctoras y obligación de información

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

2. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, este investigará inmediatamente las causas, en colaboración con el responsable del despliegue que lo haya notificado, en su caso, e informará a las autoridades de vigilancia del mercado competentes respecto al sistema de IA de alto riesgo de que se trate y, cuando proceda, al organismo notificado que haya expedido un certificado para dicho sistema de conformidad con lo dispuesto en el artículo 44, en particular sobre la naturaleza del incumplimiento y sobre cualquier medida correctora adoptada.

Artículo 21
Cooperación con las autoridades competentes

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

2. Previa solicitud motivada de una autoridad competente, los proveedores darán también a dicha autoridad, cuando proceda, acceso a los archivos de registro generados automáticamente del sistema de IA de alto riesgo a que se refiere el artículo 12, apartado 1, en la medida en que dichos archivos estén bajo su control.

3. Toda información obtenida por una autoridad competente con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 22
Representantes autorizados de los proveedores de sistemas de IA de alto riesgo

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

2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a las autoridades de vigilancia del mercado, cuando lo soliciten, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión según lo indicado por la autoridad de competente. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) verificar que se han elaborado la declaración UE de conformidad a que se refiere el artículo 47 y la documentación técnica a que se refiere el artículo 11 y que el proveedor ha llevado a cabo un procedimiento de evaluación de la conformidad adecuado;

b) conservar a disposición de las autoridades competentes y de las autoridades u organismos nacionales a que se refiere el artículo 74, apartado 10, durante un período de diez años a contar desde la introducción en el mercado o la 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 a que se refiere el artículo 47, la documentación técnica y, en su caso, el certificado expedido por el organismo notificado;

c) proporcionar a una autoridad competente, previa solicitud motivada, toda la información y la documentación, incluida la mencionada en el presente párrafo, letra b), que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, incluido el acceso a los 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;

d) cooperar con las autoridades competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que este presente;

e) cuando proceda, cumplir las obligaciones de registro a que se refiere el artículo 49, apartado 1, o si el registro lo lleva a cabo el propio proveedor, garantizar que la información a que se refiere el anexo VIII, sección A, punto 3, es correcta.

El mandato habilitará al representante autorizado para que las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene las obligaciones que le atañen con arreglo al presente Reglamento. En tal caso, además, informará de inmediato de la terminación del mandato y de los motivos de esta medida a la autoridad de vigilancia del mercado pertinente, así como, cuando proceda, al organismo notificado pertinente.

Artículo 23
Obligaciones de los importadores

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

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

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

c) el sistema lleve el marcado CE exigido y vaya acompañado de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso;

d) el proveedor haya designado a un representante autorizado de conformidad con el artículo 22, apartado 1.

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 79, apartado 1, el importador informará de ello al proveedor del sistema, a los representantes autorizados y a las autoridades de vigilancia del mercado.

3. Los importadores indicarán, en el embalaje del sistema de IA de alto riesgo o en la documentación que lo acompañe, cuando proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.

4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometan el cumplimiento de los requisitos establecidos en la sección 2 por parte de dicho sistema.

5. Los importadores conservarán, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad a que se refiere el artículo 47.

6. Los importadores proporcionarán a las autoridades competentes pertinentes, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5, que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua que estas puedan entender fácilmente. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades.

7. Los importadores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo introducido en el mercado por los importadores, en particular para reducir y mitigar los riesgos que este presente.

Artículo 24
Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE exigido, que vaya acompañado de una copia de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso, y que el proveedor y el importador de dicho sistema, según corresponda, hayan cumplido sus obligaciones establecidas en el artículo 16, letras b) y c), y el artículo 23, apartado 3, respectivamente.

2. Si un distribuidor considera o tiene motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en la sección 2, no lo comercializará hasta que se haya conseguido esa conformidad. Además, si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, 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 de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometen el cumplimiento por parte del sistema de los requisitos establecidos en la sección 2.

4. Los distribuidores que consideren o tengan motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en la sección 2 adoptarán las medidas correctoras necesarias para que sea conforme, para 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 79, apartado 1, su distribuidor informará inmediatamente de ello al proveedor o al importador del sistema y a las autoridades competentes respecto al sistema de IA de alto riesgo de que se trate y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad competente pertinente, los distribuidores de un sistema de IA de alto riesgo proporcionarán a esa autoridad toda la información y la documentación relativas a sus actuaciones con arreglo a los apartados 1 a 4 que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2.

6. Los distribuidores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo comercializado por los distribuidores, en particular para reducir o mitigar los riesgos que esté presente.

Artículo 25

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

1. Cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de IA de alto riesgo a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias:

a) cuando ponga su nombre o marca 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) cuando modifique sustancialmente un sistema de IA de alto riesgo que ya haya sido introducido en el mercado o puesto en servicio de tal manera que siga siendo un sistema de IA de alto riesgo con arreglo al artículo 6;

c) cuando modifique la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido considerado de alto riesgo y ya haya sido introducido en el mercado o puesto en servicio, de tal manera que el sistema de IA de que se trate se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

2. Cuando se den las circunstancias mencionadas en el apartado 1, el proveedor que inicialmente haya introducido en el mercado el sistema de IA o lo haya puesto en servicio dejará de ser considerado proveedor de ese sistema de IA específico a efectos del presente Reglamento. Ese proveedor inicial cooperará estrechamente con los nuevos proveedores y facilitará la información necesaria, el acceso técnico u otra asistencia razonablemente previstos que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. El presente apartado no se aplicará en los casos en que el proveedor inicial haya indicado claramente que su sistema de IA no debe ser transformado en un sistema de IA de alto riesgo y, por lo tanto, no está sujeto a la obligación de facilitar la documentación.

3. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos contemplados en los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el fabricante del producto será considerado proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en alguna de las siguientes circunstancias:

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

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

4. El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA de alto riesgo, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y otra asistencia que sean necesarios, sobre la base del estado de la técnica generalmente reconocido, para que el proveedor del sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. El presente apartado no se aplicará a terceros que pongan a disposición del público herramientas, servicios, procesos o componentes distintos de modelos de IA de uso general, en el marco de una licencia libre y de código abierto.

La Oficina de IA podrá elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo. Cuando elabore esas cláusulas contractuales tipo de carácter voluntario, la Oficina de IA tendrá en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio. Las cláusulas contractuales tipo de carácter voluntario se publicarán y estarán disponibles gratuitamente en un formato electrónico fácilmente utilizable.

5. Los apartados 2 y 3 se entenderán sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, de conformidad con el Derecho de la Unión y nacional.

Artículo 26
Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo

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

2. Los responsables del despliegue encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

3. Las obligaciones previstas en los apartados 1 y 2 no afectan a otras obligaciones que el Derecho nacional o de la Unión imponga a los responsables del despliegue ni a su libertad para organizar sus propios recursos y actividades con el fin de poner en práctica las medidas de supervisión humana que indique el proveedor.

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

5. Los responsables del despliegue vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores con arreglo al artículo 72. Cuando los responsables del despliegue tengan motivos para considerar que utilizar el sistema de IA de alto riesgo conforme a sus instrucciones puede dar lugar a que ese sistema de AI presente un riesgo en el sentido del artículo 79, apartado 1, informarán, sin demora indebida, al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso de ese sistema. Cuando los responsables del despliegue detecten un incidente grave, informarán asimismo inmediatamente de dicho incidente, en primer lugar, al proveedor y, a continuación, al importador o distribuidor y a la autoridad de vigilancia del mercado pertinente. En el caso de que el responsable del despliegue no consiga contactar con el proveedor, el artículo 73 se aplicará *mutatis mutandis*. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho.

En el caso de los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de vigilancia prevista en el párrafo primero cuando se respeten las normas sobre sistemas, procesos y mecanismos de gobernanza interna de acuerdo con el Derecho pertinente en materia de servicios financieros.

6. Los responsables del despliegue de sistemas de IA de alto riesgo conservarán los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo

que se disponga otra cosa 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 responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro como parte de la documentación conservada en virtud del Derecho de la Unión en materia de servicios financieros.

7. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, cuando proceda, con arreglo a las normas y procedimientos establecidos en el Derecho de la Unión y nacional y conforme a las prácticas en materia de información a los trabajadores y sus representantes.

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

9. Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 del presente Reglamento 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.

10. No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, *ex ante* o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

En caso de que se deniegue la autorización contemplada en el párrafo primero, dejará de utilizarse el sistema de identificación biométrica remota en diferido objeto de la solicitud de autorización con efecto inmediato y se eliminarán los datos personales asociados al uso del sistema de IA de alto riesgo para el que se solicitó la autorización.

Dicho sistema de IA de alto riego de identificación biométrica remota en diferido no se utilizará en ningún caso a los efectos de la garantía del cumplimiento del Derecho

de forma indiscriminada, sin que exista relación alguna con un delito, un proceso penal, una amenaza real y actual o real y previsible de delito, o con la búsqueda de una persona desaparecida concreta. Se velará por que las autoridades garantes del cumplimiento del Derecho no puedan adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida de dichos sistemas de identificación biométrica remota en diferido.

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

Con independencia de la finalidad o del responsable del despliegue, se documentará toda utilización de tales sistemas de IA de alto riesgo en el expediente policial pertinente y se pondrá a disposición, previa solicitud, de la autoridad de vigilancia del mercado pertinente y de la autoridad nacional de protección de datos, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. El presente párrafo se entenderá sin perjuicio de los poderes conferidas por la Directiva (UE) 2016/680 a las autoridades de control.

Los responsables del despliegue presentarán informes anuales a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos sobre el uso que han hecho de los sistemas de identificación biométrica remota en diferido, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. Los informes podrán agregarse de modo que cubran más de un despliegue.

Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota en diferido.

11. Sin perjuicio de lo dispuesto en el artículo 50 del presente Reglamento, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo que se utilicen a los efectos de la garantía del cumplimiento del Derecho, se aplicará el artículo 13 de la Directiva (UE) 2016/680.

12. Los responsables del despliegue cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el presente Reglamento.

Artículo 27

Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo

1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del desplie-

gue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. A tal fin, los responsables del despliegue llevarán a cabo una evaluación que consistirá en:

a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;

b) una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;

c) las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;

d) los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;

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

f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

2. La obligación descrita con arreglo al apartado 1 se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto riesgo, el responsable del despliegue considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.

3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, presentando el modelo cumplimentado a que se refiere el apartado 5 del presente artículo. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de esta obligación de notificación.

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

5. La Oficina de IA elaborará un modelo de cuestionario, también mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada.

SECCIÓN 4
Autoridades notificantes y organismos notificados

Artículo 28
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. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros.

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 este.

3. Las autoridades notificantes se constituirán, se organizarán y funcionarán de forma que no surjan conflictos de intereses 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 consultoría de carácter comercial o competitivo.

6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas. Cuando proceda, el personal competente tendrá los conocimientos especializados necesarios para ejercer sus funciones, en ámbitos como las tecnologías de la información, la IA y el Derecho, incluida la supervisión de los derechos fundamentales.

Artículo 29
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 los tipos de 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 31.

Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante en virtud de cualquier otro acto de la 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 periódicamente que cumple los requisitos establecidos en el artículo 31.

4. En lo que respecta a los organismos notificados designados de conformidad con cualquier otro acto legislativo 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 del presente artículo 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 31.

Artículo 30
Procedimiento de notificación

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

2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, mediante el sistema de notificación electrónica desarrollado y gestionado por la Comisión, cada organismo de evaluación de la conformidad a que se refiere el apartado 1.

3. La notificación a que se refiere el apartado 2 del presente artículo incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA afectados, así como la certificación de competencia pertinente. Si la notificación no está basada en el certificado de acreditación a que se refiere el artículo 29, 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 supervisará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 31.

4. El organismo de evaluación de la conformidad de que se trate 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 esta incluya el certificado de acreditación a que se refiere el artículo 29, apartado 2, o de dos meses tras la notificación de la autoridad notificante cuando esta incluya las pruebas documentales a que se refiere el artículo 29, apartado 3.

5. Cuando se formulen objeciones, la Comisión iniciará sin demora consultas con los Estados miembros pertinentes y el organismo de evaluación de la conformidad. En vista de todo ello, la Comisión enviará su decisión al Estado miembro afectado y al organismo de evaluación de la conformidad pertinente.

Artículo 31
Requisitos relativos a los organismos notificados

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

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

3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados ofrecerán confianza en su 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 los sistemas de IA de alto riesgo que se evalúen, así como de cualquier competidor del proveedor. Ello no será óbice para el uso de sistemas de IA de alto riesgo evaluados que sean necesarios para las actividades del organismo de evaluación de la conformidad o para el uso de tales sistemas de alto riesgo con fines personales.

5. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la comercialización o el uso de dichos sistemas de IA de alto riesgo, ni tampoco representarán a las partes que llevan a cabo estas actividades. Además, no efectuarán ninguna actividad que pudiera entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que han sido notificados. Ello se aplicará especialmente a los servicios de consultoría.

6. 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 poner en práctica los principios de imparcialidad aplicables en toda su organización, a todo su personal y en todas sus actividades de evaluación.

7. Los organismos notificados contarán con procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos mantengan, de conformidad con el artículo 78, la confidencialidad de la información que llegue a su poder en el desempeño de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija su divulgación. 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 funciones que les hayan sido encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.

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

9. 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 establecidos con arreglo al Derecho nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

10. Los organismos notificados serán capaces de llevar a cabo todas sus tareas 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.

11. Los organismos notificados contarán con competencias técnicas 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, jurídico y científico que tenga experiencia y conocimientos relativos a los tipos de sistemas de IA, los datos y la computación de datos pertinentes y a los requisitos establecidos en la sección 2.

12. 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 pertinentes.

Artículo 32
Presunción de conformidad con los requisitos relativos a los organismos notificados

Cuando un organismo de evaluación de la conformidad demuestre que cumple los criterios establecidos en las normas armonizadas pertinentes, o en partes de estas, cuyas referencias estén publicadas en el *Diario Oficial de la Unión Europea*, se presumirá que cumple los requisitos establecidos en el artículo 31 en la medida en que las normas armonizadas aplicables contemplen esos mismos requisitos.

Artículo 33

Filiales de organismos notificados y subcontratación

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 31 e informará a la autoridad notificante en consecuencia.

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

3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor. Los organismos notificados pondrán a disposición del público una lista de sus filiales.

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

Artículo 34

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 establecidos en el artículo 43.

2. Los organismos notificados evitarán cargas innecesarias para los proveedores cuando desempeñen sus actividades, y tendrán debidamente en cuenta el tamaño del proveedor, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a reducir al mínimo las cargas administrativas y los costes del cumplimiento para las microempresas y pequeñas empresas en el sentido de la Recomendación 2003/361/CE. 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 28, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, a fin de que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y de facilitar la evaluación descrita en la presente sección.

Artículo 35

Números de identificación y listas de organismos notificados

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

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, incluidos sus números de identificación 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 en la notificación de un organismo notificado a través del sistema de notificación electrónica a que se refiere el artículo 30, apartado 2.

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

Para modificaciones de la notificación distintas de las ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados 3 a 9.

3. 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, al menos un año antes de poner fin a sus actividades. Los certificados del organismo notificado 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 de alto riesgo cubiertos por dichos certificados. Este último organismo notificado realizará una evaluación completa de los sistemas de IA de alto riesgo afectados antes del vencimiento de ese plazo de nueve meses y antes de expedir nuevos certificados para esos sistemas. Si el organismo notificado ha puesto fin a sus actividades, la autoridad notificante retirará la designación.

4. Si una autoridad notificante tiene motivo suficiente para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, la autoridad notificante investigará el asunto sin demora y con la máxima diligencia. En ese contexto, informará al organismo notificado de que se trate acerca de las objeciones formuladas y le ofrecerá la posibilidad de exponer sus puntos de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, dicha autoridad limitará, suspenderá o retirará la designación, según el caso, 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.

5. Cuando su designación haya sido suspendida, limitada o retirada total o parcialmente, el organismo notificado informará a los proveedores afectados a más en un plazo de diez días.

6. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante adoptará las medidas oportunas para garantizar que los archivos del organismo

notificado de que se trate se conserven, y para ponerlos a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado, a petición de estas.

7. En caso de la 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 designación;

c) exigirá al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, todo certificado indebidamente expedido, a fin de garantizar la conformidad continua de los sistemas de IA de alto riesgo 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 cuya suspensión o retirada haya exigido; dicha autoridad tomará las medidas oportunas, cuando sea necesario, para evitar un riesgo para la salud, la seguridad o los derechos fundamentales.

8. Salvo en el caso de los certificados expedidos indebidamente, y cuando una designación haya sido suspendida o limitada, los certificados mantendrán su validez en una de 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 fijado un calendario de acciones para subsanar la suspensión o la limitación, o

b) cuando la autoridad notificante haya confirmado que no se expedirán, modificarán ni volverán a expedir certificados relacionados con la suspensión mientras dure la suspensión o limitación, y declare si el organismo notificado tiene o no la capacidad, durante el período de la suspensión o limitación, de seguir supervisando los certificados expedidos y siendo responsable de ellos; cuando la autoridad notificante determine que el organismo notificado no tiene la capacidad de respaldar los certificados expedidos, el proveedor del sistema cubierto por el certificado deberá confirmar por escrito a las autoridades nacionales competentes del Estado miembro en que tenga su domicilio social, en un plazo de tres meses a partir de la suspensión o limitación, 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.

9. Salvo en el caso de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados mantendrán su validez durante nueve meses en las circunstancias siguientes:

a) la autoridad nacional competente del Estado miembro en el que tiene su domicilio social el proveedor del sistema de IA de alto riesgo cubierto por el certificado ha confirmado que no existe ningún riesgo para la salud, la seguridad o los derechos fundamentales asociado al sistema de IA de alto riesgo de que se trate, y

b) otro organismo notificado ha confirmado por escrito que asumirá la responsabilidad inmediata de dichos sistemas de IA y completa su evaluación en el plazo de doce meses a partir de 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 tenga su domicilio social el proveedor del sistema cubierto por el certificado 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 designación informarán de ello inmediatamente a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

Artículo 37

Cuestionamiento 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 la competencia de un organismo notificado o del cumplimiento continuo, por parte de un organismo notificado, de los requisitos establecidos en el artículo 31 y de sus responsabilidades aplicables.

2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación o el mantenimiento de la competencia del organismo notificado de que se trate.

3. La Comisión garantizará el tratamiento confidencial de acuerdo con el artículo 78 de toda la información delicada 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 para su notificación, informará al Estado miembro notificante en consecuencia y le solicitará que adopte las medidas correctoras necesarias, incluidas la suspensión o la retirada de la designación en caso necesario. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión, mediante un acto de ejecución, podrá suspender, limitar o retirar la designación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

Artículo 38
Coordinación de los organismos notificados

1. La Comisión se asegurará de que se instaure y se mantenga 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. Cada autoridad notificante se asegurará de que los organismos notificados por ella participen en el trabajo del grupo a que se refiere el apartado 1, directamente o por medio de representantes designados.

3. La Comisión dispondrá que se organicen intercambios de conocimientos y mejores prácticas entre autoridades notificantes.

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 establecidos en el artículo 31 o garanticen un nivel equivalente de cumplimiento.

SECCIÓN 5
Normas, evaluación de la conformidad, certificados, registro

Artículo 40
Normas armonizadas y documentos de normalización

1. Los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con normas armonizadas, o partes de estas, cuyas referencias estén publicadas en el *Diario Oficial de la Unión Europea* de conformidad con el Reglamento (UE) n.o 1025/2012 se presumirá que son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, en su caso, con las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento, en la medida en que dichas normas contemplen estos requisitos u obligaciones.

2. De conformidad con el artículo 10 del Reglamento (UE) n.o 1025/2012, la Comisión formulará, sin demora indebida, peticiones de normalización que contemplen todos los requisitos establecidos en la sección 2 del presente capítulo y, según proceda, las peticiones de normalización que contemplen las obligaciones establecidas en el capítulo V, secciones

2 y 3, del presente Reglamento. La petición de normalización también incluirá la solicitud de documentos sobre los procesos de presentación de información y documentación a fin de mejorar el funcionamiento de los de los sistemas de IA desde el punto de vista de los recursos, como la reducción del consumo de energía y de otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, así como sobre el desarrollo eficiente desde el punto de vista energético de los modelos de IA de uso general. Cuando prepare una petición de normalización, la Comisión consultará al Consejo de IA y a las partes interesadas pertinentes, incluido el foro consultivo.

Cuando dirija una petición de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas deben ser claras, coherentes —también con las normas elaboradas en diversos sectores para los productos regulados por los actos legislativos de armonización de la Unión vigentes enumerados en el anexo I— y destinadas a garantizar que los sistemas de IA de alto riesgo o los modelos de IA de uso general introducidos en el mercado o puestos en servicio en la Unión cumplan los requisitos u obligaciones pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de que han hecho todo lo posible por cumplir los objetivos a que se refieren los párrafos primero y segundo del presente apartado, de conformidad con el artículo 24 del Reglamento (UE) n.o 1025/2012.

3. Los participantes en el proceso de normalización tratarán de promover la inversión y la innovación en IA, también incrementando la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, de contribuir al refuerzo de la cooperación mundial en pro de la normalización, teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que son coherentes con los valores, derechos fundamentales e intereses de la Unión, y de mejorar la gobernanza multilateral, garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n.o 1025/2012.

Artículo 41
Especificaciones comunes

1. La Comisión podrá adoptar actos de ejecución por los que se establezcan especificaciones comunes para los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, siempre que se hayan cumplido las siguientes condiciones:

a) la Comisión ha solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.o 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en la sección 2 del presente capítulo, o según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, y:

i) la solicitud no ha sido aceptada por ninguna de las organizaciones europeas de normalización, o

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

iii) las normas armonizadas pertinentes responden de forma insuficiente a las preocupaciones en materia de derechos fundamentales, o

iv) las normas armonizadas no se ajustan a la solicitud, y

b) no se ha publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que regulen los requisitos establecidos en la sección 2 del presente capítulo, o según proceda, las obligaciones a que se refiere el capítulo V, secciones 2 y 3, de conformidad con el Reglamento (UE) n.o 1025/2012 y no se prevé la publicación de tal referencia en un plazo razonable.

Al elaborar las disposiciones comunes, la Comisión consultará al foro consultivo a que se refiere el artículo 67.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 98, apartado 2.

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

3. Se presumirá que los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con las especificaciones comunes a que se refiere el apartado 1, o partes de dichas especificaciones, son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para cumplir con las obligaciones a que se refiere el capítulo V, secciones 2 y 3, en la medida en que dichas especificaciones comunes contemplen esos requisitos o esas obligaciones.

4. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el *Diario Oficial de la Unión Europea*, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.o 1025/2012. Cuando la referencia a una norma armonizada se publique en el *Diario Oficial de la Unión Europea*, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o las partes de dichos actos que contemplen los mismos requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, las mismas obligaciones establecidas en el capítulo V, secciones 2 y 3.

5. Cuando los proveedores de sistemas de IA de alto riesgo o los modelos de IA de uso general no cumplan las especificaciones comunes mencionadas en el apartado 1, justificarán debidamente que han adoptado soluciones técnicas que cumplan los requisitos a que se refiere la sección 2 del presente capítulo o, según corresponda, cumplan con

las obligaciones establecidas en el capítulo V, secciones 2 y 3, en un nivel como mínimo equivalente a aquellos.

6. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en la sección 2, o, según corresponda, no cumple con las obligaciones establecidas en el capítulo V, secciones 2 y 3, informará de ello a la Comisión con una explicación detallada. La Comisión evaluará dicha información y, en su caso, modificará el acto de ejecución por el que se establece la especificación común de que se trate.

Artículo 42
Presunción de conformidad con determinados requisitos

1. Se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto su uso cumplen los requisitos pertinentes establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que cuenten con un certificado o una declaración de conformidad en virtud de un esquema de ciberseguridad con arreglo al Reglamento (UE) 2019/881 cuyas referencias estén publicadas 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, contemplen dichos requisitos.

Artículo 43
Evaluación de la conformidad

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

a) el fundamentado en el control interno, mencionado en el anexo VI, o

b) el 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.

Al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor se atendrá al procedimiento de evaluación de la conformidad establecido en el anexo VII cuando:

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

b) el proveedor no haya aplicado la norma armonizada, o solo haya aplicado parte de esta;

c) existan las especificaciones comunes a que se refiere la letra a), pero el proveedor no las haya aplicado;

d) una o varias de las normas armonizadas a que se refiere la letra a) se hayan publicado con una limitación, y únicamente en la parte de la norma objeto de la limitación.

A efectos del procedimiento de evaluación de la conformidad mencionado en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema de IA de alto riesgo por parte de las autoridades garantes del cumplimiento del Derecho, las autoridades de inmigración o las autoridades de asilo, o por las instituciones, órganos u organismos de la Unión, la autoridad de vigilancia del mercado mencionada en el artículo 74, apartado 8 o 9, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, 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 regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el proveedor se atendrá al procedimiento de evaluación de la conformidad pertinente exigida por dichos actos legislativos. Los requisitos establecidos en la sección 2 del presente capítulo se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. Asimismo, se aplicarán los puntos 4.3, 4.4 y 4.5 del anexo VII, así como el punto 4.6, párrafo quinto, de dicho anexo.

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 la sección 2, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11, en el contexto del procedimiento de notificación con arreglo a dichos actos legislativos.

Cuando un acto legislativo enumerado en el anexo I, sección A, permita al fabricante del producto prescindir de una evaluación de la conformidad de terceros, a condición de que el fabricante haya aplicado todas las normas armonizadas que contemplan todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado las normas armonizadas o, en su caso, las especificaciones comunes a que se refiere el artículo 41 que contemplan todos los requisitos establecidos en la sección 2 del presente capítulo.

4. Los sistemas de IA de alto riesgo que ya hayan sido objeto de un procedimiento de evaluación de la conformidad se someterán a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue actual.

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 en la información recogida en la documentación técnica mencionada en el anexo IV, punto 2, letra f), no constituirán modificaciones sustanciales.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar los anexos VI y VII actualizándolos a la luz del progreso técnico.

6. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar los apartados 1 y 2 del presente artículo a fin de someter a los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, 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 mencionado 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 pertinentes del Estado miembro en el que esté establecido el organismo notificado puedan entender fácilmente.

2. Los certificados serán válidos para el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales no superiores a cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado mantendrá su validez a condición de que 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 la sección 2, 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.

Existirá un procedimiento de recurso frente a las decisiones de los organismos notificados, también respecto a los certificados de conformidad expedidos.

Artículo 45
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, de cualquier suplemento a dichos certificados y de cualesquiera aprobaciones de sistemas de gestión de la calidad expedidas con arreglo a los requisitos establecidos 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 expedida con arreglo a los requisitos establecidos en el anexo VII;

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

d) de cualquier 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 aplicación de su notificación y de cualquier otra actividad realizada, incluidas 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 gestión de la calidad que haya expedido;

b) de los certificados de la Unión de evaluación de la documentación técnica 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 tipos de sistemas de IA información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de las evaluaciones de la conformidad.

4. Los organismos notificados preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

Artículo 46
Exención del procedimiento de evaluación de la conformidad

1. Como excepción a lo dispuesto en el artículo 43 y previa solicitud debidamente motivada, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo específicos en el territorio del

Estado miembro de que se trate por motivos excepcionales de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras. Dicha autorización se concederá por un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, teniendo en cuenta los motivos excepcionales que justifiquen la exención. La conclusión de los procedimientos de que se trate se alcanzará sin demora indebida.

2. En una situación de urgencia debidamente justificada por motivos excepcionales de seguridad pública o en caso de amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, las autoridades garantes del cumplimiento del Derecho 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 se solicite dicha autorización durante o después de la utilización sin demora indebida. Si se deniega la autorización a que se refiere el apartado 1, se suspenderá el uso del sistema de IA de alto riesgo con efecto inmediato y se desecharán inmediatamente todos los resultados y toda la información de salida producidos por dicho uso.

3. 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 la sección 2. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida de conformidad con los apartados 1 y 2. Esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho.

4. Si, en el plazo de quince días naturales tras la recepción de la información indicada en el apartado 3, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una autorización expedida por una autoridad de vigilancia del mercado de un Estado miembro con arreglo al apartado 1, la autorización se considerará justificada.

5. Si, en el plazo de quince días naturales tras la recepción de la notificación a que se refiere el apartado 3, un Estado miembro formula objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o si la Comisión considera que la autorización vulnera el Derecho de la Unión o que la conclusión de los Estados miembros relativa al cumplimiento del sistema a que se refiere el apartado 3 es infundada, la Comisión celebrará consultas con el Estado miembro pertinente sin demora. Se consultará a los operadores de que se trate y se les ofrecerá la posibilidad de exponer sus puntos de vista. En vista de todo ello, la Comisión decidirá si la autorización está justificada o no. La Comisión enviará su decisión al Estado miembro afectado y a los operadores pertinentes.

6. Si la Comisión considera que la autorización no está justificada, la autoridad de vigilancia del mercado del Estado miembro de que se trate la retirará.

7. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, solo se aplicarán las exenciones de la evaluación de la conformidad establecidas en dichos actos legislativos de armonización de la Unión.

Artículo 47
Declaración UE de conformidad

1. El proveedor redactará una declaración UE de conformidad por escrito en un formato legible por máquina, con firma electrónica o manuscrita, para cada sistema de IA de alto riesgo y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a contar desde la introducción del sistema de IA de alto riesgo en el mercado o su puesta en servicio. En la declaración UE de conformidad se especificará el sistema de IA de alto riesgo 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 establecidos en la sección 2. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a una lengua que puedan entender fácilmente las autoridades nacionales competentes del Estado o Estados miembros en que se introduzca en el mercado o comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sujetos a otros actos legislativos de armonización de la Unión que también exijan una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos el Derecho de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para determinar los actos legislativos de armonización de la Unión a los que se refiere la declaración.

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

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo V actualizando el contenido de la declaración UE de conformidad establecida en dicho anexo, con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

Artículo 48
Marcado CE

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

2. En el caso de los sistemas de IA de alto riesgo que se proporcionan digitalmente, se utilizará un marcado CE digital, únicamente si es fácilmente accesible a través de la interfaz desde la que se accede a dicho sistema o mediante un código fácilmente accesible legible por máquina u otros medios electrónicos.

3. 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.

4. En su caso, el marcado CE irá seguido del número de identificación del organismo notificado responsable de los procedimientos de evaluación de la conformidad establecidos en el artículo 43. El número de identificación del organismo notificado lo colocará él mismo o, siguiendo sus instrucciones, el proveedor o el representante autorizado del proveedor. 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.

5. Cuando los sistemas de IA de alto riesgo estén sujetos a otras disposiciones del Derecho de la Unión que también requieran la colocación del marcado CE, este indicará que los sistemas de IA de alto riesgo también cumplen los requisitos de esas otras disposiciones.

Artículo 49
Registro

1. Antes de introducir en el mercado o de poner en servicio 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, punto 2, el proveedor o, en su caso, el representante autorizado, registrarán su sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

2. Antes de introducir en el mercado o poner en servicio un sistema de IA sobre el que el proveedor haya llegado a la conclusión de que no es de alto riesgo de conformidad con el artículo 6, apartado 3, dicho proveedor o, en su caso, el representante autorizado, registrarán ese sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

3. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE a que se refiere el artículo 71.

4. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1, 2 y 3 del presente artículo se efectuará en una sección segura no pública de la base de datos de la UE a que se refiere el artículo 71 e incluirá únicamente la información, según proceda, a la que se hace referencia en:

a) el anexo VIII, sección A, puntos 1 a 10, con excepción de los puntos 6, 8 y 9;

b) el anexo VIII, sección B, puntos 1 a 5 y puntos 8 y 9;

c) el anexo VIII, sección C, puntos 1 a 3;

d) el anexo IX, puntos 1, 2, 3 y 5.

Únicamente la Comisión y las autoridades nacionales a que se refiere el artículo 74, apartado 8, tendrán acceso a las secciones restringidas respectivas de la base de datos de la UE enumeradas en el párrafo primero del presente apartado.

5. Los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, se registrarán a nivel nacional.

CAPÍTULO IV

OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE DETERMINADOS SISTEMAS DE IA

Artículo 50

Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar un delito penal.

2. Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica, o cuando estén autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos.

3. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680, según corresponda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión.

4. Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. Esta obligación no se aplicará cuando la ley autorice su uso para para detectar, prevenir, investigar o enjuiciar delitos. Cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra.

Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar delitos, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido.

5. La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas de que se trate de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables.

6. Los apartados 1 a 4 no afectarán a los requisitos y obligaciones establecidos en el capítulo III y se entenderán sin perjuicio de otras obligaciones de transparencia establecidas en el Derecho nacional o de la Unión para los responsables del despliegue de sistemas de IA.

7. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión para promover la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados de manera artificial. La Comisión podrá adoptar actos de ejecución a fin de aprobar dichos códigos de buenas prácticas, de conformidad con el procedimiento establecido en el artículo 56, apartado 6. Si considera que el código no es adecuado, la Comisión podrá adoptar un acto de ejecución que especifique normas comunes para el cumplimiento de las citadas obligaciones de conformidad con el procedimiento de examen establecido en el artículo 98, apartado 2.

CAPÍTULO V
MODELOS DE IA DE USO GENERAL

SECCIÓN 1
Reglas de clasificación

Artículo 51
Reglas de clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgo sistémico

1. Un modelo de IA de uso general se clasificará como modelo de IA de uso general con riesgo sistémico si reúne alguna de las siguientes condiciones:

a) tiene capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia;

b) con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, tiene capacidades o un impacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.

2. Se presumirá que un modelo de IA de uso general tiene capacidades de gran impacto con arreglo al apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 1025.

3. La Comisión adoptará actos delegados de conformidad con el artículo 97 para modificar los umbrales a que se refieren los apartados 1 y 2 del presente artículo, así como para complementar los parámetros de referencia e indicadores en función de los avances tecnológicos, como las mejoras algorítmicas o la mayor eficiencia del hardware, cuando sea necesario, para que los umbrales reflejen el estado actual de la técnica.

Artículo 52
Procedimiento

1. Cuando un modelo de IA de uso general cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), el proveedor pertinente lo notificará a la Comisión sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse. Dicha notificación incluirá la información necesaria para demostrar que se cumple el requisito pertinente. Si la Comisión tiene conocimiento de un modelo de IA de uso general que presenta riesgos sistémicos y que no ha sido notificado, podrá decidir designarlo como modelo con riesgo sistémico.

2. El proveedor de un modelo de IA de uso general que cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados que demuestren que, excepcionalmente,

aunque el modelo de IA de uso general cumple dicho requisito, no presenta riesgos sistémicos, debido a sus características específicas, y no debe clasificarse, por tanto, como modelo de IA de uso general con riesgo sistémico.

3. Cuando la Comisión concluya que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y que el proveedor pertinente no ha sido capaz de demostrar que el modelo de IA de uso general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos y el modelo de IA de uso general se considerará un modelo de IA de uso general con riesgo sistémico.

4. La Comisión podrá determinar que un modelo de IA de uso general presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada del grupo de expertos científicos con arreglo al artículo 90, apartado 1, letra a), a partir de los criterios establecidos en el anexo XIII.

La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar el anexo XIII especificando y actualizando los criterios establecidos en dicho anexo.

5. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos con arreglo a los criterios establecidos en el anexo XIII. Dicha solicitud contendrá motivos objetivos, detallados y nuevos que hayan surgido desde la decisión de designación. Los proveedores no podrán solicitar la reevaluación antes de transcurridos seis meses desde la decisión de designación. Si tras la reevaluación la Comisión decide mantener la designación como modelo de IA de uso general con riesgo sistémico, los proveedores no podrán solicitar otra reevaluación hasta transcurridos seis meses desde dicha decisión.

6. La Comisión velará por que se publique una lista de modelos de IA de uso general con riesgo sistémico, que mantendrá actualizada, sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

SECCIÓN 2

Obligaciones de los proveedores de modelos de IA de uso general

Artículo 53

Obligaciones de los proveedores de modelos de IA de uso general

1. Los proveedores de modelos de IA de uso general:

a) elaborarán y mantendrán actualizada la documentación técnica del modelo, incluida la información relativa al proceso de entrenamiento y realización de pruebas y los resultados de su evaluación, que contendrá, como mínimo, la información establecida en el anexo XI con el fin de facilitarla, previa solicitud, a la Oficina de IA y a las autoridades nacionales competentes;

b) elaborarán y mantendrán actualizada información y documentación y la pondrán a disposición de los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas de IA. Sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, dicha información y documentación:

   i) permitirá a los proveedores de sistemas de IA entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones en virtud del presente Reglamento, y

   ii) contendrá, como mínimo, los elementos previstos en el anexo XII;

c) establecerán directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines, y en particular, para detectar y cumplir, por ejemplo, a través de tecnologías punta, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

d) elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA.

2. Las obligaciones establecidas en el apartado 1, letras a) y b), no se aplicarán a los proveedores de modelos de IA que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de uso general con riesgo sistémico.

3. Los proveedores de modelos de IA de uso general cooperarán con la Comisión y las autoridades nacionales competentes, según sea necesario, en el ejercicio de sus competencias y facultades en virtud del presente Reglamento.

4. Los proveedores de modelos de IA de uso general podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

5. A fin de facilitar el cumplimiento de lo dispuesto en el anexo XI, en particular en su punto 2, letras d) y e), la Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 para detallar las metodologías de medición y cálculo con vistas a que la documentación sea comparable y verificable.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97, apartado 2, para modificar los anexos XI y XII en función de los avances tecnológicos.

7. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 54
Representantes autorizados de los proveedores de modelos de IA de uso general

1. Antes de introducir en el mercado de la Unión un modelo de IA de uso general, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a la Oficina de IA, cuando lo solicite, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) comprobar que se ha elaborado la documentación técnica que se indica en el anexo XI y que el proveedor cumple todas las obligaciones a que se refiere el artículo 53 y, en su caso, el artículo 55;

b) conservar una copia de la documentación técnica que se indica en el anexo XI a disposición de la Oficina de IA y de las autoridades nacionales competentes por un período de diez años a partir de la introducción en el mercado del modelo de IA de uso general, y de los datos de contacto del proveedor que haya designado al representante autorizado;

c) facilitar a la Oficina de IA, previa solicitud motivada, toda la información y documentación, incluidas la información y documentación mencionadas en la letra b), que sean necesarias para demostrar el cumplimiento de las obligaciones establecidas en el presente capítulo;

d) cooperar con la Oficina de IA y las autoridades competentes, previa solicitud motivada, en cualquier acción que emprendan en relación con el modelo de IA de uso general, también cuando el modelo esté integrado en un sistema de IA introducido en el mercado o puesto en servicio en la Unión.

4. El mandato habilitará al representante autorizado para que la Oficina de IA o las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

5. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene sus obligaciones en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de IA del fin del mandato y de los motivos para ello.

6. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de uso general que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, salvo si los citados modelos de IA de uso general presentan riesgos sistémicos.

SECCIÓN 3

Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

Artículo 55

Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

1. Además de las obligaciones enumeradas en los artículos 53 y 54, los proveedores de modelos de IA de uso general con riesgo sistémico:

a) evaluarán los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación de adversarios con el modelo con vistas a detectar y mitigar riesgos sistémicos;

b) evaluarán y mitigarán los posibles riesgos sistémicos a escala de la Unión que puedan derivarse del desarrollo, la introducción en el mercado o el uso de modelos de IA de uso general con riesgo sistémico, así como el origen de dichos riesgos;

c) vigilarán, documentarán y comunicarán, sin demora indebida, a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos;

d) velarán por que se establezca un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémico y la infraestructura física del modelo.

2. Los proveedores de modelos de IA de uso general con riesgo sistémico podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida

en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

3. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

SECCIÓN 4
Códigos de buenas prácticas

Artículo 56
Códigos de buenas prácticas

1. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión a fin de contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.

2. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas comprendan al menos las obligaciones establecidas en los artículos 53 y 55, entre las que se incluyen las cuestiones siguientes:

a) los medios para garantizar que la información a que se refiere el artículo 53, apartado 1, letras a) y b), se mantenga actualizada con respecto a la evolución del mercado y los avances tecnológicos;

b) el nivel adecuado de detalle por lo que respecta al resumen sobre el contenido utilizado para el entrenamiento;

c) la determinación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluido su origen, cuando proceda;

d) las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionales a los riesgos y tendrán en cuenta su gravedad y probabilidad y las dificultades específicas para hacerles frente, habida cuenta de la manera en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.

3. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán contribuir al proceso.

4. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, como,

por ejemplo, indicadores clave de rendimiento, si procede, para garantizar la consecución de dichos objetivos, y que tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.

5. La Oficina de IA velará por que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de IA sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, lo que incluye su evaluación con respecto a los indicadores clave de rendimiento, si procede. Los indicadores clave de rendimiento y los compromisos de presentación de información reflejarán las diferencias de tamaño y capacidad entre los distintos participantes.

6. La Oficina de IA y el Consejo de IA supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Oficina de IA y el Consejo de IA evaluarán si los códigos de buenas prácticas incluyen las obligaciones establecidas en los artículos 53 y 55, y supervisarán y evaluarán periódicamente la consecución de sus objetivos. Publicarán su evaluación de la adecuación de los códigos de buenas prácticas.

La Comisión podrá, mediante un acto de ejecución, aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

7. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los códigos de buenas prácticas. En el caso de los proveedores de modelos de IA de uso general que no presenten riesgos sistémicos, esta adhesión podrá limitarse a las obligaciones previstas en el artículo 53, salvo que declaren expresamente su interés en adherirse al código completo.

8. La Oficina de IA también fomentará y facilitará, según proceda, la revisión y la adaptación de los códigos de buenas prácticas, en particular teniendo en cuenta las normas emergentes. La Oficina de IA asistirá en la evaluación de las normas disponibles.

9. Los códigos de buenas prácticas estarán finalizados a más tardar el 2 de mayo de 2025. La Oficina de IA adoptará las medidas necesarias, lo que incluye invitar a los proveedores a adherirse a los códigos de buenas prácticas con arreglo a lo dispuesto en el apartado 7.

Si un código de buenas prácticas no se ha podido finalizar a más tardar el 2 de agosto de 2025, o si la Oficina de IA lo considera inadecuado tras su evaluación con arreglo al apartado 6 del presente artículo, la Comisión podrá establecer, mediante actos de ejecución, normas comunes para el cumplimiento de las obligaciones establecidas en los artículos 53 y 55, que incluyan las cuestiones establecidas en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO VI
MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 57
Espacios controlados de pruebas para la IA

1. Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2026. Dicho espacio controlado de pruebas también podrá establecerse conjuntamente con las autoridades competentes de otros Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento y herramientas para el establecimiento y el funcionamiento de los espacios controlados de pruebas para la IA.

La obligación prevista en el párrafo primero también podrá cumplirse mediante la participación en un espacio controlado de pruebas existente en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente a los Estados miembros participantes.

2. También podrán establecerse espacios controlados de pruebas para la IA adicionales a escala regional o local o conjuntamente con las autoridades competentes de otros Estados miembros.

3. El Supervisor Europeo de Protección de Datos también podrá establecer un espacio controlado de pruebas para la IA para las instituciones, órganos y organismos de la Unión, y podrá ejercer las funciones y tareas de las autoridades nacionales competentes de conformidad con el presente capítulo.

4. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 2 asignen recursos suficientes para cumplir lo dispuesto en el presente artículo de manera efectiva y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA. El presente artículo no afectará a otros espacios controlados de pruebas establecidos en virtud del Derecho de la Unión o nacional. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros espacios controlados de pruebas y las autoridades nacionales competentes.

5. Los espacios controlados de pruebas para la IA establecidos de conformidad con el apartado 1 proporcionarán un entorno controlado que fomente la innovación y facilite el desarrollo, el entrenamiento, la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio, con arreglo a un plan del espacio controlado de pruebas específico acordado entre los proveedores o proveedores potenciales y la autoridad competente. Tales espacios controlados de pruebas podrán incluir pruebas en condiciones reales supervisadas dentro de ellos.

6. Las autoridades competentes proporcionarán, en su caso, orientación, supervisión y apoyo dentro del espacio controlado de pruebas para la IA con vistas a determinar

los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, a las pruebas y a las medidas de reducción y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, cuando proceda, de otras disposiciones de Derecho de la Unión y nacional cuya observancia se supervise en el espacio controlado de pruebas.

7. Las autoridades competentes proporcionarán a los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA orientaciones sobre las expectativas en materia de regulación y la manera de cumplir los requisitos y obligaciones establecidos en el presente Reglamento.

A petición del proveedor o proveedor potencial del sistema de IA, la autoridad competente aportará una prueba escrita de las actividades llevadas a cabo con éxito en el espacio controlado de pruebas. La autoridad competente también proporcionará un informe de salida en el que se detallen las actividades llevadas a cabo en el espacio controlado de pruebas y los resultados y resultados del aprendizaje correspondientes. Los proveedores podrán utilizar esta documentación para demostrar su cumplimiento del presente Reglamento mediante el proceso de evaluación de la conformidad o las actividades de vigilancia del mercado pertinentes. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán en cuenta positivamente los informes de salida proporcionados y las pruebas escritas aportadas por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

8. Con sujeción a las disposiciones de confidencialidad del artículo 78 y con el acuerdo del proveedor o proveedor potencial, la Comisión y el Consejo 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 proveedor o proveedor potencial como la autoridad nacional competente dan expresamente su acuerdo para ello, el informe de salida podrá hacerse público a través de la plataforma única de información a que se refiere el presente artículo.

9. El establecimiento de espacios controlados de pruebas para la IA tendrá por objeto contribuir a los siguientes objetivos:

a) mejorar la seguridad jurídica para lograr el cumplimiento del presente Reglamento o, en su caso, de otras disposiciones de Derecho de la Unión y nacional aplicable;

b) apoyar el intercambio de mejores prácticas mediante la cooperación con las autoridades que participan en el espacio controlado de pruebas para la IA;

c) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de la IA;

d) contribuir a un aprendizaje normativo basado en datos contrastados;

e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los proporcionen pymes, incluidas las empresas emergentes.

10. Las autoridades nacionales competentes velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes

que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos y las demás autoridades nacionales o competentes estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias.

11. Los espacios controlados de pruebas para la IA no afectarán a las facultades de supervisión o correctoras de las autoridades competentes que supervisan los espacios controlados de pruebas, tampoco a escala regional o local. Cualquier riesgo considerable para la salud, la seguridad y los derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas de IA dará lugar a una reducción adecuada. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de prueba, o la participación en el espacio controlado de pruebas si no es posible una reducción efectiva, e informarán a la Oficina de IA de dicha decisión. Con el objetivo de apoyar la innovación en materia de IA en la Unión, las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites del Derecho pertinente y harán uso de su potestad discrecional a la hora de aplicar disposiciones jurídicas en relación con un proyecto específico de espacio controlado de pruebas para la IA.

12. Los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA responderán, con arreglo al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas. Sin embargo, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones proporcionadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del presente Reglamento. En los casos en que otras autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA en el espacio controlado de pruebas y hayan proporcionado orientaciones para el cumplimiento, no se impondrán multas administrativas en relación con dichas disposiciones.

13. Los espacios controlados de pruebas para la IA serán diseñados y puestos en práctica de tal manera que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.

14. Las autoridades nacionales competentes coordinarán sus actividades y cooperarán en el marco del Consejo de IA.

15. Las autoridades nacionales competentes informarán a la Oficina de IA y al Consejo de IA del establecimiento de un espacio controlado de pruebas y podrán solicitarles apoyo y orientación. La Oficina de IA pondrá a disposición del público una lista de los espacios controlados de pruebas previstos y existentes y la mantendrá actualizada con el fin de fomentar una mayor interacción en los espacios controlados de pruebas para la IA, así como la cooperación transfronteriza.

16. Las autoridades nacionales competentes presentarán informes anuales a la Oficina de IA y al Consejo de IA, por primera vez un año después del establecimiento del espacio controlado de pruebas para la IA y, posteriormente, cada año hasta su terminación, así

como un informe final. Dichos informes proporcionarán información sobre el progreso y los resultados de la puesta en práctica de dichos espacios controlados de pruebas, incluidos mejores prácticas, incidentes, enseñanzas extraídas y recomendaciones acerca de su configuración y, en su caso, acerca de la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y sobre la aplicación de otras disposiciones de Derecho de la Unión, supervisada por las autoridades competentes en el marco del espacio controlado de pruebas. Las autoridades nacionales competentes pondrán dichos informes anuales, o resúmenes de estos, a disposición del público, en línea. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones en virtud del presente Reglamento.

17. La Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los espacios controlados de pruebas para la IA para que las partes interesadas puedan interactuar con los espacios controlados de pruebas para la IA y plantear consultas a las autoridades competentes, así como pedir orientaciones no vinculantes sobre la conformidad de productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 62, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda.

Artículo 58

Disposiciones detalladas relativas a los espacios controlados de pruebas para la IA y al funcionamiento de dichos espacios

1. A fin de evitar que se produzca una fragmentación en la Unión, la Comisión adoptará actos de ejecución que especifiquen las disposiciones detalladas para el establecimiento, el desarrollo, la puesta en práctica, el funcionamiento y la supervisión de los espacios controlados de pruebas para la IA. Los actos de ejecución incluirán principios comunes sobre las siguientes cuestiones:

a) los criterios de admisibilidad y selección para participar en el espacio controlado de pruebas para la IA;

b) los procedimientos para la solicitud, la participación, la supervisión, la salida y la terminación del espacio controlado de pruebas para la IA, incluidos el plan del espacio controlado de pruebas y el informe de salida;

c) las condiciones aplicables a los participantes.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. Los actos de ejecución mencionados en el apartado 1 garantizarán:

a) que los espacios controlados de pruebas para la IA estén abiertos a cualquier proveedor o proveedor potencial de un sistema de IA que presente una solicitud y cumpla los criterios de admisibilidad y selección, que serán transparentes y equitativos, y también que las autoridades nacionales competentes informen a los solicitantes de su decisión en un plazo de tres meses a partir de la presentación de la solicitud;

b) que los espacios controlados de pruebas para la IA permitan un acceso amplio e igualitario y se adapten a la demanda de participación; los proveedores y proveedores potenciales también podrán presentar solicitudes en asociación con responsables del despliegue y con otros terceros pertinentes;

c) que las disposiciones detalladas y las condiciones relativas a los espacios controlados de pruebas para la IA propicien, en la medida de lo posible, que las autoridades nacionales competentes dispongan de flexibilidad para establecer y gestionar sus espacios controlados de pruebas para la IA;

d) que el acceso a los espacios controlados de pruebas para la IA sea gratuito para las pymes, incluidas las empresas emergentes, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de una forma justa y proporcionada;

e) que se facilite a los proveedores y proveedores potenciales, mediante los resultados del aprendizaje de los espacios controlados de pruebas para la IA, el cumplimiento de las obligaciones de evaluación de la conformidad en virtud del presente Reglamento y la aplicación voluntaria de los códigos de conducta a que se refiere el artículo 95;

f) que los espacios controlados de pruebas para la IA faciliten la participación de otros agentes pertinentes del ecosistema de la IA, como los organismos notificados y los organismos de normalización, las pymes, incluidas las empresas emergentes, las empresas, los agentes innovadores, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación y los centros europeos de innovación digital, los centros de excelencia y los investigadores, a fin de permitir y facilitar la cooperación con los sectores público y privado;

g) que los procedimientos, procesos y requisitos administrativos para la solicitud, la selección, la participación y la salida del espacio controlado de pruebas para la IA sean sencillos y fácilmente inteligibles y se comuniquen claramente, a fin de facilitar la participación de las pymes, incluidas las empresas emergentes, con capacidades jurídicas y administrativas limitadas, y se racionalicen en toda la Unión, a fin de evitar la fragmentación y de que la participación en un espacio controlado de pruebas para la IA establecido por un Estado miembro o por el Supervisor Europeo de Protección de Datos esté reconocida mutua y uniformemente y tenga los mismos efectos jurídicos en toda la Unión;

h) que la participación en el espacio controlado de pruebas para la IA se limite a un período que se ajuste a la complejidad y la escala del proyecto, y que podrá ser prorrogado por la autoridad nacional competente;

i) que los espacios controlados de pruebas para la IA faciliten el desarrollo de herramientas e infraestructuras para la prueba, la evaluación comparativa, la evaluación y la explicación de las dimensiones de los sistemas de IA pertinentes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como de medidas para mitigar los riesgos para los derechos fundamentales y la sociedad en su conjunto.

3. Se ofrecerán a los proveedores potenciales que participen en los espacios controlados de pruebas para la IA, en particular a las pymes y las empresas emergentes, cuando proceda, servicios previos al despliegue, como orientaciones sobre la aplicación del presente Reglamento, otros servicios que aportan valor añadido, como ayuda con los documentos de normalización y la certificación, y acceso a las instalaciones de ensayo y experimentación, los centros europeos de innovación digital y los centros de excelencia.

4. Cuando las autoridades nacionales competentes estudien autorizar la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA que se establecerá en virtud del presente artículo, acordarán específicamente las condiciones de dichas pruebas y, en particular, las garantías adecuadas con los participantes, 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 59

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

1. En el espacio controlado de pruebas, los datos personales recabados lícitamente con otros fines podrán tratarse únicamente con el objetivo de desarrollar, entrenar y probar determinados sistemas de IA en el espacio controlado de pruebas cuando se cumplan todas las condiciones siguientes:

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

   i) la seguridad y la salud públicas, incluidos la detección, el diagnóstico, la prevención, el control y el tratamiento de enfermedades y la mejora de los sistemas sanitarios,

   ii) un elevado nivel de protección y mejora de la calidad del medio ambiente, la protección de la biodiversidad, la protección contra la contaminación, las medidas de transición ecológica, la mitigación del cambio climático y las medidas de adaptación a este,

   iii) la sostenibilidad energética,

   iv) la seguridad y la resiliencia de los sistemas de transporte y la movilidad, las infraestructuras críticas y las redes,

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

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

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

d) que 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 del proveedor potencial, y que únicamente las personas autorizadas tengan acceso a dichos datos;

e) que los proveedores solo puedan compartir los datos recabados originalmente de conformidad con el Derecho de la Unión en materia de protección de datos; los datos personales creados en el espacio controlado de pruebas no pueden salir del espacio controlado de pruebas;

f) que el tratamiento de datos personales en el contexto del espacio controlado de pruebas no dé lugar a medidas o decisiones que afecten a los interesados ni afecte a la aplicación de sus derechos establecidos en el Derecho de la Unión en materia de protección de datos personales;

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, salvo que se disponga otra cosa en el Derecho de la Unión o el Derecho nacional;

i) que se conserve una descripción completa y detallada del proceso y la lógica subyacentes al 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 comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo.

2. Cuando se lleve a cabo con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, y bajo el control y la responsabilidad de las autoridades garantes del cumplimiento del Derecho, el tratamiento de datos personales en los espacios controlados de pruebas para la IA se basará en un Derecho específico, de la Unión o nacional y cumplirá las condiciones acumulativas que se indican en el apartado 1.

3. El apartado 1 se entiende sin perjuicio del Derecho de la Unión o nacional que proscriba el tratamiento de datos personales con fines distintos de los expresamente mencionados en dichos actos, así como sin perjuicio del Derecho de la Unión o nacional que establezca las bases para el tratamiento de datos personales necesario para desarrollar, probar o entrenar sistemas innovadores de IA o de cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales.

Artículo 60

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

1. Los proveedores o proveedores potenciales de sistemas de IA de alto riesgo enumerados en el anexo III podrán realizar pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA de conformidad el presente artículo y con el plan de la prueba en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.

La Comisión adoptará, mediante un acto de ejecución, los elementos detallados del plan de la prueba en condiciones reales. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

El presente apartado se entiende sin perjuicio del Derecho de la Unión o nacional en materia de pruebas en condiciones reales de sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I.

2. Los proveedores o proveedores potenciales podrán realizar pruebas de los sistemas de IA de alto riesgo mencionados 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 asociación con uno o varios responsables del despliegue o responsables del despliegue potenciales.

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

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

a) el proveedor o proveedor potencial ha elaborado un plan de la prueba en condiciones reales y lo ha presentado a la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales;

b) la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales ha aprobado las pruebas en condiciones reales y el plan de la prueba en condiciones reales; si la autoridad de vigilancia del mercado no responde en un plazo de treinta días, se entenderá que las pruebas en condiciones

reales y el plan de la prueba en condiciones reales han sido aprobados; cuando el Derecho nacional no contemple una aprobación tácita, las pruebas en condiciones reales estarán sujetas a una autorización también en este caso;

c) el proveedor o proveedor potencial, con excepción de los proveedores o proveedores potenciales de sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, así como de los sistemas de IA de alto riesgo mencionados en el punto 2 del anexo III ha registrado las pruebas en condiciones reales de conformidad con el artículo 71, apartado 4, con un número de identificación único para toda la Unión y la información indicada en el anexo IX; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, ha registrado las pruebas en condiciones reales en la parte no pública de la base de datos de la UE de conformidad con el artículo 49, apartado 4, letra d), con un número de identificación único para toda la Unión y la información indicada en este; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, ha registrado las pruebas en condiciones reales de conformidad con el artículo 49, apartado 5;

d) el proveedor o proveedor potencial que realiza las pruebas en condiciones reales está establecido en la Unión o ha designado a un representante legal que está establecido en la Unión;

e) los datos recabados y tratados a efectos de las pruebas en condiciones reales únicamente se transferirán a terceros países si se aplican las garantías adecuadas y aplicables en virtud del Derecho de la Unión;

f) las pruebas en condiciones reales no duran más de lo necesario para lograr sus objetivos y, en cualquier caso, no más de seis meses, que podrán prorrogarse por un período adicional de seis meses, con sujeción al envío de una notificación previa por parte del proveedor o proveedor potencial a la autoridad de vigilancia del mercado, acompañada por una explicación de la necesidad de dicha prórroga;

g) los sujetos de las pruebas en condiciones reales que sean personas pertenecientes a colectivos vulnerables debido a su edad o a una discapacidad cuentan con protección adecuada;

h) cuando un proveedor o proveedor potencial organice las pruebas en condiciones reales en cooperación con uno o varios responsables del despliegue o responsables del despliegue potenciales, estos últimos habrán sido informados de todos los aspectos de las pruebas que resulten pertinentes para su decisión de participar y habrán recibido las instrucciones de uso pertinentes del sistema de IA a que se refiere el artículo 13; el proveedor o proveedor potencial y el responsable del despliegue o responsable del despliegue potencial alcanzarán un acuerdo en que se detallen sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a las pruebas en condiciones reales con arreglo al presente Reglamento y a otras disposiciones de Derecho de la Unión y nacional aplicable;

i) los sujetos de las pruebas en condiciones reales han dado su consentimiento informado de conformidad con el artículo 61 o, en el ámbito de la garantía del cumplimiento del Derecho, en el que intentar obtener el consentimiento informado impediría que se probara el sistema de IA, las pruebas en sí y los resultados de las pruebas en condiciones reales no tendrán ningún efecto negativo sobre los sujetos, cuyos datos personales se suprimirán una vez realizada la prueba;

j) las pruebas en condiciones reales son supervisadas de manera efectiva por el proveedor o el proveedor potencial y por los responsables del despliegue o los responsables del despliegue potenciales mediante personas adecuadamente cualificadas en el ámbito pertinente y con la capacidad, formación y autoridad necesarias para realizar sus tareas;

k) se pueden revertir y descartar de manera efectiva las predicciones, recomendaciones o decisiones del sistema de IA.

5. Cualquier sujeto de las pruebas en condiciones reales o su representante legalmente designado, según proceda, podrá, sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación, abandonar las pruebas en cualquier momento retirando su consentimiento informado y solicitar la supresión inmediata y permanente de sus datos personales. La retirada del consentimiento informado no afectará a las actividades ya completadas.

6. De conformidad con el artículo 75, los Estados miembros conferirán a sus autoridades de vigilancia del mercado poderes para exigir a los proveedores y proveedores potenciales que faciliten información, realizar sin previo aviso inspecciones a distancia o *in situ* y controlar la realización de las pruebas en condiciones reales y los sistemas de IA de alto riesgo relacionados. Las autoridades de vigilancia del mercado harán uso de dichos poderes para garantizar que las pruebas en condiciones reales se desarrollen de manera segura.

7. Se informará de cualquier incidente grave detectado en el transcurso de las pruebas en condiciones reales a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 73. El proveedor o proveedor potencial adoptará medidas de reducción inmediatas o, en su defecto, suspenderá las pruebas en condiciones reales hasta que se produzca dicha reducción o pondrá fin a las pruebas. El proveedor o proveedor potencial establecerá un procedimiento para la rápida recuperación del sistema de IA en caso de que se ponga fin a las pruebas en condiciones reales.

8. El proveedor o proveedor potencial notificará a la autoridad nacional de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales la suspensión o la terminación de las pruebas en condiciones reales y los resultados finales.

9. El proveedor o proveedor potencial será responsable, conforme al Derecho de la Unión y nacional en materia de responsabilidad aplicable, de cualquier daño causado en el transcurso de sus pruebas en condiciones reales.

Artículo 61

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

1. A los efectos de las pruebas en condiciones reales con arreglo al artículo 60, se obtendrá de los sujetos de las pruebas un consentimiento informado dado libremente antes de participar en dichas pruebas y después de haber recibido información concisa, clara, pertinente y comprensible en relación con:

a) la naturaleza y los objetivos de las pruebas en condiciones reales y los posibles inconvenientes asociados a su participación;

b) las condiciones en las que se van a llevar a cabo las pruebas en condiciones reales, incluida la duración prevista de la participación del sujeto o los sujetos;

c) sus derechos y las garantías relativas a su 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;

d) las disposiciones para solicitar la reversión o el descarte de las predicciones, recomendaciones o decisiones del sistema de IA;

e) el número de identificación único para toda la Unión de la prueba en condiciones reales de conformidad con el artículo 60, apartado 4, letra c), y la información de contacto del proveedor o de su representante legal, de quien se puede obtener más información.

2. El consentimiento informado estará fechado y documentado, y se entregará una copia a los sujetos de la prueba o a sus representantes legales.

Artículo 62

Medidas dirigidas a proveedores y responsables del despliegue, en particular pymes, incluidas las empresas emergentes

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionarán a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección; el acceso prioritario no impedirá que otras pymes, incluidas las empresas emergentes, distintas de las mencionadas en el presente apartado accedan al espacio controlado de pruebas para la IA, siempre que también cumplan las condiciones de admisibilidad y los criterios de selección;

b) organizarán actividades de sensibilización y formación específicas sobre la aplicación del presente Reglamento adaptadas a las necesidades de las pymes, incluidas las empresas emergentes, los responsables del despliegue y, en su caso, las autoridades públicas locales;

c) utilizarán canales específicos existentes y establecerán, en su caso, nuevos canales para la comunicación con las pymes, incluidas las empresas emergentes, los responsables del despliegue y otros agentes innovadores, así como, en su caso, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las dudas planteadas acerca de la aplicación del presente Reglamento, también en relación con la participación en los espacios controlados de pruebas para la IA;

d) fomentarán la participación de las pymes y otras partes interesadas pertinentes en el proceso de desarrollo de la normalización.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores que sean pymes, incluidas las 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 Oficina de IA adoptará las medidas siguientes:

a) proporcionará modelos normalizados para los ámbitos regulados por el presente Reglamento, tal como especifique el Consejo de IA en su solicitud;

b) desarrollará y mantendrá una plataforma única de información que proporcione información fácil de usar en relación con el presente Reglamento destinada a todos los operadores de la Unión;

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

d) evaluará y fomentará la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

Artículo 63
Excepciones para operadores específicos

1. Las microempresas en el sentido de la Recomendación 2003/361/CE podrán cumplir determinados elementos del sistema de gestión de la calidad exigido por el artículo 17 del presente Reglamento de manera simplificada, siempre que no tengan empresas asociadas o empresas vinculadas en el sentido de dicha Recomendación. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que puedan cumplirse de manera simplificada teniendo en cuenta las necesidades de las microempresas sin que ello afecte al nivel de protección ni a la necesidad de cumplir los requisitos relativos a los sistemas de IA de alto riesgo.

2. El apartado 1 del presente artículo no se interpretará en el sentido de que exime a dichos operadores de cumplir cualquier otro requisito u obligación establecidos en el presente Reglamento, incluidos aquellos que figuran en los artículos 9, 10, 11, 12, 13, 14, 15, 72 y 73.

CAPÍTULO VII
GOBERNANZA

SECCIÓN 1
Gobernanza a escala de la Unión

Artículo 64
Oficina de IA

1. La Comisión desarrollará los conocimientos especializados y las capacidades de la Unión en el ámbito de la IA mediante la Oficina de IA.

2. Los Estados miembros facilitarán las tareas encomendadas a la Oficina de IA, que están reflejadas en el presente Reglamento.

Artículo 65
Creación y estructura del Consejo Europeo de Inteligencia Artificial

1. Se crea un Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»).

2. El Consejo de IA estará compuesto de un representante por Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de IA también asistirá a las reuniones del Consejo de IA sin participar en las votaciones. El Consejo de IA podrá invitar a otras autoridades, organismos o expertos nacionales y de la Unión a las reuniones en función de cada situación concreta, cuando los temas tratados sean relevantes para ellos.

3. Cada representante será designado por su Estado miembro por un período de tres años, renovable una vez.

4. Los Estados miembros se asegurarán de que sus representantes en el Consejo de IA:

a) tengan las competencias y los poderes pertinentes en su Estado miembro para poder contribuir activamente al cumplimiento de las funciones del Consejo de IA a que se refiere el artículo 66;

b) sean designados como punto de contacto único respecto del Consejo de IA y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

c) estén facultados para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes en su Estado miembro en relación con la aplicación del presente Reglamento, también mediante la recopilación de datos e información pertinentes para cumplir sus funciones en el Consejo de IA.

5. Los representantes designados de los Estados miembros adoptarán el Reglamento Interno del Consejo de IA por mayoría de dos tercios. El Reglamento Interno establecerá, en particular, los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las funciones de la presidencia, las modalidades de votación detalladas y la organización de las actividades del Consejo de IA y de sus subgrupos.

6. El Consejo de IA establecerá dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y de notificar a las autoridades cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. Cuando proceda, se podrá invitar a representantes del foro consultivo a que se refiere el artículo 67 a dichos subgrupos o a reuniones específicas de dichos subgrupos en calidad de observadores.

7. El Consejo de IA se organizará y gestionará de manera que se preserve la objetividad e imparcialidad de sus actividades.

8. El Consejo de IA estará presidido por uno de los representantes de los Estados miembros. La Oficina de IA asumirá las labores de secretaría del Consejo de IA, convocará las reuniones a petición de la presidencia y elaborará el orden del día de conformidad con las funciones del Consejo de IA en virtud del presente Reglamento y de su Reglamento Interno.

Artículo 66
Funciones del Consejo de IA

El Consejo de IA prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, el Consejo de IA podrá, en particular:

a) contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación con las autoridades de vigilancia del mercado de que se trate y previo acuerdo de estas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartado 11;

b) recopilar y compartir conocimientos técnicos y reglamentarios y mejores prácticas entre los Estados miembros;

c) ofrecer asesoramiento sobre la aplicación del presente Reglamento, en particular en lo relativo al cumplimiento de las normas sobre modelos de IA de uso general;

d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, también en relación con la exención de los procedimientos de evaluación de la

conformidad a que se refiere el artículo 46, el funcionamiento de los espacios controlados de pruebas para la IA y las pruebas en condiciones reales a que se refieren los artículos 57, 59 y 60;

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

   i) sobre la elaboración y aplicación de códigos de conducta y códigos de buenas prácticas con arreglo al presente Reglamento, así como de las directrices de la Comisión,

   ii) sobre la evaluación y revisión del presente Reglamento con arreglo al artículo 112, también en lo que respecta a los informes de incidentes graves a que se refiere el artículo 73, y el funcionamiento de la base de datos de la UE a que se refiere el artículo 71, la preparación de los actos delegados o de ejecución, y en lo que respecta a las posibles adaptaciones del presente Reglamento a los actos legislativos de armonización de la Unión enumerados en el anexo I,

   iii) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el capítulo III, sección 2,

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

   v) sobre tendencias, como la competitividad de Europa a escala mundial en materia de IA, la adopción de la IA en la Unión y el desarrollo de capacidades digitales,

   vi) sobre tendencias en la tipología cambiante de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de rendición de cuentas,

   vii) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7 y sobre la posible necesidad de revisar el artículo 5 con arreglo al artículo 112, teniendo en cuenta las pruebas disponibles pertinentes y los últimos avances tecnológicos;

f) apoyar a la Comisión en la promoción de la alfabetización en materia de IA, la sensibilización del público y la comprensión de las ventajas, los riesgos, las salvaguardias y los derechos y obligaciones en relación con la utilización de sistemas de IA;

g) facilitar el desarrollo de criterios comunes y la comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, por ejemplo, contribuyendo al desarrollo de parámetros de referencia;

h) cooperar, en su caso, con otras instituciones, órganos y organismos de la Unión, así como con grupos de expertos y redes pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores, y la protección de datos y de los derechos fundamentales;

i) contribuir a la cooperación efectiva con las autoridades competentes de terceros países y con organizaciones internacionales;

j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos técnicos y organizativos necesarios para la aplicación del presente Reglamento, por ejemplo, contribuyendo a la evaluación de las necesidades de formación del personal de los Estados miembros que participe en dicha aplicación;

k) asistir a la Oficina de IA en el apoyo a las autoridades nacionales competentes para el establecimiento y el desarrollo de espacios controlados de pruebas para la IA, y facilitar la cooperación y el intercambio de información entre espacios controlados de pruebas para la IA;

l) contribuir a la elaboración de documentos de orientación y proporcionar el asesoramiento pertinente al respecto;

m) proporcionar asesoramiento a la Comisión en relación con asuntos internacionales en materia de IA;

n) emitir dictámenes para la Comisión sobre las alertas cualificadas relativas a modelos de IA de uso general;

o) recibir dictámenes de los Estados miembros sobre alertas cualificadas relativas a modelos de IA de uso general y sobre las experiencias y prácticas nacionales en materia de supervisión y ejecución de los sistemas de IA, en particular los sistemas que integran los modelos de IA de uso general.

Artículo 67
Foro consultivo

1. Se creará un foro consultivo para proporcionar conocimientos técnicos y asesorar al Consejo de IA y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento.

2. La composición del foro consultivo representará una selección equilibrada de partes interesadas, incluidos la industria, las empresas emergentes, las pymes, la sociedad civil y el mundo académico. La composición del foro consultivo estará equilibrada en lo que respecta a los intereses comerciales y los no comerciales y, dentro de la categoría de los intereses comerciales, en lo que respecta a las pymes y otras empresas.

3. La Comisión nombrará a los miembros del foro consultivo, de conformidad con los criterios establecidos en el apartado 2, de entre las partes interesadas con conocimientos especializados reconocidos en el ámbito de la IA.

4. El mandato de los miembros del foro consultivo será de dos años y podrá prorrogarse hasta un máximo de cuatro años.

5. La Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) serán miembros permanentes del foro consultivo.

6. El foro consultivo establecerá su reglamento interno. Elegirá dos copresidentes de entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una sola vez.

7. El foro consultivo celebrará reuniones al menos dos veces al año. Podrá invitar a expertos y otras partes interesadas a sus reuniones.

8. El foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones por escrito a petición del Consejo de IA o de la Comisión.

9. El foro consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.

10. El foro consultivo redactará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

Artículo 68
Grupo de expertos científicos independientes

1. La Comisión adoptará, mediante un acto de ejecución, disposiciones sobre la creación de un grupo de expertos científicos independientes (en lo sucesivo, «grupo de expertos científicos») destinado a apoyar las actividades de garantía del cumplimiento previstas en el presente Reglamento. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. El grupo de expertos científicos estará compuesto por expertos seleccionados por la Comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA necesarios para las funciones establecidas en el apartado 3, y será capaz de demostrar que cumple todas las condiciones siguientes:

a) conocimientos especializados y competencias particulares, y conocimientos científicos o técnicos en el ámbito de la IA;

b) independencia de cualquier proveedor de sistemas de IA o de modelos de IA de uso general;

c) capacidad para llevar a cabo actividades con diligencia, precisión y objetividad.

La Comisión, en consulta con el Consejo de IA, determinará el número de expertos del grupo de acuerdo con las necesidades requeridas y garantizará una representación geográfica y de género justa.

3. El grupo de expertos científicos asesorará y apoyará a la Oficina de IA, en particular en lo que respecta a las siguientes funciones:

a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los sistemas y modelos de IA de uso general, en particular:

   i) alertando a la Oficina de IA de los posibles riesgos sistémicos a escala de la Unión de modelos de IA de uso general, de conformidad con el artículo 90,

ii) contribuyendo al desarrollo de herramientas y metodologías para evaluar las capacidades de los sistemas y modelos de IA de uso general, también a través de parámetros de referencia,

iii) asesorando sobre la clasificación de modelos de IA de uso general con riesgo sistémico,

iv) asesorando sobre la clasificación de diversos sistemas y modelos de IA de uso general,

v) contribuyendo al desarrollo de herramientas y modelos;

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

c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el artículo 74, apartado 11, sin perjuicio de los poderes de las autoridades de vigilancia del mercado;

d) apoyar a la Oficina de IA en el ejercicio de sus funciones en el contexto del procedimiento de salvaguardia de la Unión con arreglo al artículo 81.

4. Los expertos del grupo desempeñarán sus funciones con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones previstas en el apartado 3. Cada experto cumplimentará una declaración de intereses que se hará pública. La Oficina de IA establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, los procedimientos y las disposiciones detalladas para que el grupo de expertos científicos y sus miembros emitan alertas y soliciten la asistencia de la Oficina de IA para el desempeño de las funciones del grupo de expertos científicos.

Artículo 69

Acceso a expertos por parte de los Estados miembros

1. Los Estados miembros podrán recurrir a expertos del grupo de expertos científicos para que apoyen sus actividades de garantía del cumplimiento previstas en el presente Reglamento.

2. Se podrá exigir a los Estados miembros que paguen tasas por el asesoramiento y el apoyo prestado por los expertos. La estructura y el importe de las tasas, así como la escala y la estructura de los costes recuperables, se establecerán en el acto de ejecución a que se refiere el artículo 68, apartado 1, teniendo en cuenta los objetivos de la correcta aplicación del presente Reglamento, la rentabilidad y la necesidad de garantizar que todos los Estados miembros tengan un acceso efectivo a los expertos.

3. La Comisión facilitará el acceso oportuno de los Estados miembros a los expertos, según sea necesario, y garantizará que la combinación de las actividades de apoyo llevadas

a cabo por las estructuras de apoyo a los ensayos de IA de la Unión con arreglo al artículo 84 y por expertos con arreglo al presente artículo se organice de manera eficiente y ofrezca el mayor valor añadido posible.

SECCIÓN 2
Autoridades nacionales competentes

Artículo 70
Designación de las autoridades nacionales competentes y de los puntos de contacto único

1. 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. Dichas autoridades nacionales competentes ejercerán sus poderes de manera independiente, imparcial y sin sesgos, a fin de preservar la objetividad de sus actividades y funciones y de garantizar la aplicación y ejecución del presente Reglamento. Los miembros de dichas autoridades se abstendrán de todo acto incompatible con sus funciones. Siempre que se respeten esos principios, tales actividades y funciones podrán ser realizadas por una o varias autoridades designadas, de conformidad con las necesidades organizativas del Estado miembro.

2. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público, por medios de comunicación electrónica, información sobre la forma de contactar con las autoridades competentes y los puntos de contacto únicos a más tardar el 2 de agosto de 2025. Los Estados miembros designarán una autoridad de vigilancia del mercado que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto. La Comisión pondrá a disposición del público la lista de puntos de contacto únicos.

3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.

4. Las autoridades nacionales competentes adoptarán las medidas adecuadas para garantizar un nivel adecuado de ciberseguridad.

5. En el desempeño de sus funciones, las autoridades nacionales competentes actuarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

6. A más tardar el 2 de agosto de 2025 y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Consejo de IA para que mantenga un debate sobre ella y, en su caso, formule recomendaciones.

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

8. Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento sobre la aplicación del presente Reglamento, en particular a las pymes —incluidas las empresas emergentes—, teniendo en cuenta las orientaciones y el asesoramiento del Consejo de IA y de la Comisión, según proceda. Siempre que una autoridad nacional competente tenga la intención de proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otros actos del Derecho de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dichos actos, según proceda.

9. Cuando las instituciones, órganos 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.

CAPÍTULO VIII
BASE DE DATOS DE LA UE PARA SISTEMAS DE IA DE ALTO RIESGO

Artículo 71
Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO III

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contendrá la información mencionada en los apartados 2 y 3 del presente artículo en relación con los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados con arreglo a los artículos 49 y 60 y los sistemas de IA que no se consideren de alto riesgo en virtud del artículo 6, apartado 3, y que estén registrados con arreglo al artículo 6, apartado 4, y al artículo 49. La Comisión consultará a los expertos pertinentes a la hora de fijar las especificaciones funcionales de dicha base de datos y al Consejo de IA a la hora de actualizarlas.

2. Los datos enumerados en el anexo VIII, secciones A y B, serán introducidos en la base de datos de la UE por el proveedor o, en su caso, por el representante autorizado.

3. Los datos enumerados en el anexo VIII, sección C, serán introducidos en la base de datos de la UE por el responsable del despliegue que sea una autoridad pública, órgano u organismo, o actúe en su nombre, de conformidad con el artículo 49, apartados 3 y 4.

4. A excepción de la sección a que se refieren el artículo 49, apartado 4, y el artículo 60, apartado 4, letra c), la información presente en la base de datos de la UE y registrada de conformidad con lo dispuesto en el artículo 49 será accesible y estará a disposición del público de manera sencilla. Debe ser fácil navegar por la información y esta ha de ser legible por máquina. Únicamente podrán acceder a la información registrada de conformidad con el artículo 60 las autoridades de vigilancia de mercado y la Comisión, a menos que el proveedor potencial o el proveedor hayan dado su consentimiento a que la información también esté accesible para el público.

5. La base de datos de la UE únicamente contendrá datos personales en la medida en que sean necesarios para la recogida y el tratamiento de información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro de sistema y que cuenten con autoridad legal para representar al proveedor o al responsable del despliegue, según proceda.

6. 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, proveedores potenciales y responsables del despliegue. La base de datos de la UE cumplirá los requisitos de accesibilidad aplicables.

CAPÍTULO IX

VIGILANCIA POSCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN Y VIGILANCIA DEL MERCADO

SECCIÓN 1

Vigilancia poscomercialización

Artículo 72

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 la naturaleza de las tecnologías de IA y a los riesgos de los sistemas de IA de alto riesgo.

2. El sistema de vigilancia poscomercialización recopilará, documentará y analizará de manera activa y sistemática los datos pertinentes que pueden facilitar los responsables del despliegue o que pueden recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y que permiten al proveedor evaluar el cumplimiento permanente de los requisitos establecidos en el capítulo III,

sección 2, por parte de los sistemas de IA. Cuando proceda, la vigilancia poscomercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue que sean autoridades garantes del cumplimiento del Derecho.

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 a más tardar el 2 de febrero de 2026. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando ya se hayan establecido un sistema y un plan de vigilancia poscomercialización con arreglo a dichos actos, con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los elementos necesarios descritos en los apartados 1, 2 y 3, utilizando el modelo a que se refiere el apartado 3, en los sistemas y planes que ya existan en virtud de dicha legislación, siempre que alcance un nivel de protección equivalente.

El párrafo primero del presente apartado también se aplicará a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, introducidos en el mercado o puestos en servicio por entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros.

SECCIÓN 2
Intercambio de información sobre incidentes graves

Artículo 73
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 en los que se haya producido dicho incidente.

2. La notificación a que se refiere el apartado 1 se efectuará inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave.

El plazo para la notificación a que se refiere el párrafo primero tendrá en cuenta la magnitud del incidente grave.

3. No obstante lo dispuesto en el apartado 2 del presente artículo, en caso de una infracción generalizada o de un incidente grave tal como se define en el artículo 3, punto 49, letra b), la notificación a que se refiere el apartado 1 del presente artículo se realizará de manera inmediata y a más tardar dos días después de que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente.

4. No obstante lo dispuesto en el apartado 2, en caso de fallecimiento de una persona, la notificación se efectuará de manera inmediata después de que el proveedor o el responsable del despliegue haya establecido —o tan pronto como sospeche— una relación causal entre el sistema de IA de alto riesgo y el incidente grave, en un plazo no superior a diez días a contar de la fecha en la que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente grave.

5. Cuando sea necesario para garantizar la notificación en tiempo oportuno, el proveedor o, en su caso, el responsable del despliegue podrá presentar inicialmente una notificación incompleta, seguida de una notificación completa.

6. Después de notificar un incidente grave con arreglo al apartado 1, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación de riesgos del incidente y las medidas correctoras.

El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado afectado durante las investigaciones a que se refiere el párrafo primero, y no emprenderá acción alguna que suponga la modificación del sistema de IA afectado de un modo que pueda repercutir en cualquier evaluación posterior de las causas del incidente sin haber informado antes de dicha acción a las autoridades competentes.

7. Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente.

8. La autoridad de vigilancia del mercado adoptará medidas adecuadas tal como se establece en el artículo 19 del Reglamento (UE) 2019/1020, en un plazo de siete días a partir de la fecha en que reciba la notificación a que se refiere el apartado 1 del presente artículo, y seguirá los procedimientos de notificación previstos en dicho Reglamento.

9. En el caso de los sistemas de IA de alto riesgo a que se refiere el anexo III, introducidos en el mercado o puestos en servicio por proveedores que estén sujetos a instrumentos legislativos de la Unión por los que se establezcan obligaciones de información equivalentes a las establecidas en el presente Reglamento, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c).

10. 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 los Reglamento

(UE) 2017/745 y (UE) 2017/746, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c), del presente Reglamento, y se hará a la autoridad nacional competente elegida para tal fin por los Estados miembros en los que se haya producido el incidente.

11. Las autoridades nacionales competentes informarán de inmediato a la Comisión de todo incidente grave, independientemente de han adoptado medidas al respecto, de conformidad con el artículo 20 del Reglamento (UE) 2019/1020.

SECCIÓN 3
Garantía del cumplimiento

Artículo 74
Vigilancia del mercado y control de los sistemas de IA en el mercado de la Unión

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA regulados por el presente Reglamento. A efectos de garantía del cumplimiento efectivo 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 mencionados en el artículo 2, apartado 1, 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 anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes de cualquier información recabada en el transcurso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. Asimismo, informarán anualmente a la Comisión sobre el recurso a prácticas prohibidas que se hayan producido durante ese año y sobre las medidas adoptadas.

3. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos legislativos.

Como excepción a lo dispuesto en el párrafo primero, en circunstancias adecuadas, los Estados miembros podrán designar otra autoridad pertinente como autoridad de vigilancia del mercado, siempre que se garantice la coordinación con las autoridades sectoriales de

vigilancia del mercado pertinentes responsables de la ejecución de los actos legislativos de armonización de la Unión enumerados en el anexo I.

4. Los procedimientos a que se refieren los artículos 79 a 83 del presente Reglamento no se aplicarán a los sistemas de IA asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando dichos actos legislativos ya prevean procedimientos que garanticen un nivel equivalente de protección que tengan el mismo objetivo. En dichos casos, se aplicarán los procedimientos sectoriales pertinentes.

5. Sin perjuicio de los poderes de las autoridades de vigilancia del mercado en virtud del artículo 14 del Reglamento (UE) 2019/1020, a efectos de garantizar la ejecución efectiva del presente Reglamento, las autoridades de vigilancia del mercado podrán ejercer a distancia los poderes a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento, según proceda.

6. 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 el Derecho de la Unión en materia de servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad nacional pertinente responsable de la supervisión financiera de dichas entidades con arreglo a 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.

7. Como excepción a lo dispuesto en el apartado 6, en las circunstancias apropiadas 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 establecido por el Reglamento (UE)

n.o 1024/2013 deberán comunicar sin demora al Banco Central Europeo toda información obtenida 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.

8. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la

independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial.

9. Cuando las instituciones, órganos 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, salvo en relación con el Tribunal de Justicia de la Unión Europea cuando actúe en el ejercicio de su función judicial.

10. 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 indicada en el anexo I o en otras disposiciones de Derecho de la Unión que pudieran resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

11. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo bien las autoridades de vigilancia del mercado, bien las autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar u ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA prestará apoyo de coordinación a las investigaciones conjuntas.

12. Sin perjuicio de los poderes previstos en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

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

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 capítulo III, sección 2, y

b) se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes.

14. Cualesquiera información o documentación obtenidas por las autoridades de vigilancia del mercado se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 75

Asistencia mutua, vigilancia del mercado y control de sistemas de IA de uso general

1. Cuando un sistema de IA se base en un modelo de IA de uso general y un mismo proveedor desarrolle tanto el modelo como el sistema, la Oficina de IA estará facultada para vigilar y supervisar el cumplimiento por parte de dicho sistema de IA de las obligaciones en virtud del presente Reglamento. Para llevar a cabo estas tareas de vigilancia y supervisión, la Oficina de IA tendrá todos los poderes de una autoridad prevista en la presente sección y en el Reglamento (UE) 2019/1020.

2. Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de uso general que pueden ser utilizados directamente por los responsables del despliegue al menos para una de las finalidades clasificadas como de alto riesgo con arreglo al presente Reglamento no cumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento e informarán al respecto al Consejo de IA y las demás autoridades de vigilancia del mercado.

3. Cuando una autoridad de vigilancia del mercado no pueda concluir su investigación sobre el sistema de IA de alto riesgo por no poder acceder a determinada información relativa al modelo de IA de uso general, a pesar de haber realizado todos los esfuerzos adecuados para obtener esa información, podrá presentar una solicitud motivada a la Oficina de IA para que se imponga el acceso a dicha información. En tal caso, la Oficina de IA facilitará a la autoridad solicitante sin demora y, en cualquier caso en un plazo de treinta días, toda la información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades de vigilancia del mercado preservarán la confidencialidad de la información obtenida de conformidad con lo dispuesto en el artículo 78 del presente Reglamento. Se aplicará *mutatis mutandis* el procedimiento previsto en el capítulo VI del Reglamento (UE) 2019/1020.

Artículo 76

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

1. Las autoridades de vigilancia del mercado tendrán las competencias 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 supervisadas dentro de un espacio controlado de pruebas para la IA con arreglo al artículo 58, las autoridades de vigilancia del mercado verificarán el cumplimiento de del artículo 60 como parte de su función supervisora en el espacio controlado de pruebas para la IA. Dichas autoridades podrán permitir, según proceda, que el proveedor o proveedor potencial lleve a cabo pruebas en condiciones reales, como excepción a las condiciones establecidas en el artículo 60, apartado 4, letras f) y g).

3. Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o un tercero de un incidente grave o tenga otros motivos para pensar que no se cumplen las condiciones establecidas en los artículos 60 y 61, podrá adoptar una 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 proveedor potencial y al responsable del despliegue o responsable del despliegue potencial que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 60, apartado 4, letra b), la decisión o la objeción deberá estar motivada e indicar las vías de que dispone el proveedor o proveedor potencial para poder impugnar la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3, comunicará los motivos de dicha decisión a las autoridades de vigilancia del mercado de los demás Estados miembros en que se haya probado el sistema de IA de conformidad con el plan de la prueba.

Artículo 77
Poderes de las autoridades encargadas de proteger los derechos fundamentales

1. 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, incluido 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 cualquier documentación creada o conservada con arreglo al presente Reglamento y de acceder a ella, en un lenguaje y formato accesibles, cuando el acceso a dicha documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción. La autoridad u organismo público pertinente informará sobre cualquier solicitud de este tipo a la autoridad de vigilancia del mercado del Estado miembro que corresponda.

2. A más tardar el 2 de noviembre de 2024, cada Estado miembro designará las autoridades u organismos públicos a que se refiere el apartado 1 y los incluirá en una lista que pondrá a disposición del público. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

3. Cuando la documentación mencionada en el apartado 1 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión en materia de protección de los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 1 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para 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.

4. Cualquier información o documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 1 del presente artículo con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 78.

Artículo 78
Confidencialidad

1. La Comisión, las autoridades de vigilancia del mercado, los organismos notificados y cualquier otra persona física o jurídica que participe en la aplicación del presente Reglamento, de conformidad con el Derecho de la Unión o nacional, respetarán 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 e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos mencionados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo [1];

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

c) los intereses de seguridad pública y nacional;

d) el desarrollo de las causas penales o los procedimientos administrativos;

e) la información clasificada con arreglo al Derecho de la Unión o nacional.

2. Las autoridades involucradas en la aplicación del presente Reglamento de conformidad con el apartado 1 solo solicitarán los datos que sean estrictamente necesarios para la evaluación del riesgo que presentan los sistemas de IA y para el ejercicio de sus competencias de conformidad con el presente Reglamento y con el Reglamento (UE) 2019/1020. Establecerán medidas adecuadas y eficaces en materia de ciberseguridad a fin de proteger la seguridad y la confidencialidad de la información y los datos obtenidos, y suprimirán los datos recopilados tan pronto como dejen de ser necesarios para los fines para los que se obtuvieron, de conformidad con el Derecho de la Unión y nacional aplicable.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, la información intercambiada de forma confidencial entre las autoridades nacionales competentes o entre estas y la

---

1 Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al responsable del despliegue cuando las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo utilicen los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, y dicha divulgación comprometería los intereses de seguridad pública y nacional. Este intercambio de información no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo.

Cuando las autoridades garantes del cumplimiento del Derecho, de la inmigración o del asilo sean proveedores de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, 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 74, apartados 8 y 9, 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 una habilitación de seguridad del nivel adecuado.

4. Los apartados 1, 2 y 3 no afectarán a los derechos u obligaciones de la Comisión, los Estados miembros y sus autoridades pertinentes, ni a los derechos u obligaciones de los organismos notificados en lo que se refiere al intercambio de información y la difusión de advertencias, también en el contexto de la cooperación transfronteriza, ni a las obligaciones de facilitar información en virtud del Derecho penal de los Estados miembros que incumban a las partes interesadas.

5. Cuando sea necesario y con arreglo a las disposiciones pertinentes de los acuerdos internacionales y comerciales, la Comisión y los Estados miembros podrán intercambiar información confidencial con autoridades reguladoras de terceros países con las que hayan celebrado acuerdos de confidencialidad bilaterales o multilaterales que garanticen un nivel de confidencialidad adecuado.

Artículo 79
Procedimiento aplicable a escala nacional a los sistemas de IA que presenten un riesgo

1. Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo» tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riegos que afecten a 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 mencionado en el apartado 1 del presente artículo, 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. Debe prestarse una especial atención a los sistemas de IA que

presenten un riesgo para los colectivos vulnerables. Cuando se detecten 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 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1.

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda.

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 del presente apartado.

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 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 o su puesta en servicio, para retirar el producto o el sistema de IA independiente 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 a que se refiere el apartado 5 incluirá todos los detalles disponibles, en particular la información necesaria para la identificación del sistema de IA no conforme, el origen del sistema de IA y la cadena de suministro, la naturaleza de la presunta no conformidad y el riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos expresados por el operador correspondiente. En concreto, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno o varios de los motivos siguientes:

a) el no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5;

b) el incumplimiento de los requisitos establecidos en el capítulo III, sección 2, por parte de un sistema de IA de alto riesgo;

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

d) el incumplimiento del artículo 50.

7. Las autoridades de vigilancia del mercado 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 en relación con la no conformidad del sistema de IA de que se trate 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 mencionada en el apartado 5 del presente artículo, ninguna autoridad de vigilancia del mercado de un Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por una autoridad de vigilancia del mercado de otro 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 de tres meses a que se refiere el presente apartado se reducirá a treinta días en caso de no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 del presente Reglamento.

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

Artículo 80

Procedimiento aplicable a los sistemas de IA clasificados por el proveedor como no de alto riesgo en aplicación del anexo III

1. Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA que el proveedor haya clasificado como no de alto riesgo con arreglo al artículo 6, apartado 3, sí lo es, dicha autoridad realizará una evaluación del sistema de IA de que se trate por cuanto se refiere a su clasificación como sistema de IA de alto riesgo en función de las condiciones establecidas en el artículo 6, apartado 3, y las directrices de la Comisión.

2. Cuando, al realizar dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA afectado es de alto riesgo, pedirá sin demora indebida al proveedor correspondiente que adopte todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en el plazo que la autoridad de vigilancia del mercado podrá determinar.

3. Cuando la autoridad de vigilancia del mercado considere que la utilización del sistema de IA afectado no se circunscribe 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 exigido al proveedor que adopte.

4. El proveedor se asegurará de que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones que se establecen en el presente Reglamento. Cuando el proveedor de un sistema de IA afectado no haga lo necesario para que cumpla dichos requisitos y obligaciones en el plazo a que se refiere el apartado 2 del presente artículo, se le impondrán multas de conformidad con el artículo 99.

5. El proveedor se asegurará de que se adopten todas las medidas correctoras adecuadas para todos los sistemas de IA afectados que haya comercializado en toda la Unión.

6. Cuando el proveedor del sistema de IA afectado no adopte las medidas correctoras adecuadas en el plazo a que se refiere el apartado 2 del presente artículo, se aplicará el artículo 79, apartados 5 a 9.

7. Cuando, al realizar la evaluación con arreglo al apartado 1 del presente artículo, la autoridad de vigilancia del mercado determine que el proveedor había clasificado erróneamente el sistema de IA como de no alto riesgo con el fin de eludir la aplicación de los requisitos establecidos en el capítulo III, sección 2, se impondrán multas al proveedor de conformidad con el artículo 99.

8. En el ejercicio de su facultad de supervisión de la aplicación del presente artículo, y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar los controles pertinentes, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 71 del presente Reglamento.

Artículo 81
Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación a que se refiere el artículo 79, apartado 5, o en el plazo de treinta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, la autoridad de vigilancia del mercado de un Estado miembro formule objeciones sobre una medida adoptada por otra autoridad de vigilancia del mercado, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora indebida con la autoridad de vigilancia del mercado del Estado miembro pertinente y el operador u operadores, y evaluará la medida nacional. Basándose en los resultados de la mencionada evaluación, la Comisión decidirá, en un plazo de seis meses a partir de la notificación a que se refiere el artículo 79, apartado 5, o de sesenta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, si la medida nacional está justificada y notificará su decisión a la autoridad de vigilancia del mercado del Estado miembro interesado. La Comisión informará también a las demás autoridades de vigilancia del mercado de su decisión.

2. Cuando la Comisión considere que la medida adoptada por el Estado miembro correspondiente está justificada, todos los Estados miembros se asegurarán de adoptar las medidas restrictivas adecuadas con respecto al sistema de IA de que se trate, como exigir la retirada del sistema de IA de su mercado sin demora indebida, e informarán de ello a la Comisión. Cuando la Comisión considere que la medida nacional no está justificada, el Estado miembro correspondiente 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 82
Sistemas de IA conformes que presenten un riesgo

1. Si, tras efectuar una evaluación con arreglo a lo dispuesto en el artículo 79 y consultar a la autoridad pública nacional a que se refiere el artículo 77, apartado 1, la autoridad de vigilancia del mercado de un Estado miembro concluye que un sistema de IA de alto riesgo, a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo para la salud o la seguridad de las personas, para los derechos fundamentales o para otros aspectos de protección del interés público, pedirá al operador interesado que adopte todas las medidas adecuadas para garantizar 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 sin demora indebida, dentro de un plazo que dicha autoridad podrá determinar.

2. El proveedor u otro operador pertinente se asegurará de que se adoptan medidas correctoras con respecto a todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. Los Estados miembros informarán inmediatamente a la Comisión y a los demás Estados miembros cuando se llegue a una conclusión en virtud del apartado 1. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para detectar el sistema de IA afectado y para determinar su origen y cadena de suministro, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión entablará sin demora indebida consultas con los Estados miembros afectados y los operadores pertinentes y evaluará las medidas nacionales adoptadas. Basándose en los resultados de esta evaluación, la Comisión decidirá si la medida está justificada y, en su caso, propondrá otras medidas adecuadas.

5. La Comisión comunicará inmediatamente su decisión a los Estados miembros afectados y a los operadores pertinentes. Informará asimismo a los demás Estados miembros.

Artículo 83
Incumplimiento formal

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

a) se ha colocado el marcado CE contraviniendo el artículo 48;

b) no se ha colocado el marcado CE;

c) no se ha elaborado la declaración UE de conformidad con el artículo 47;

d) no se ha elaborado correctamente la declaración UE de conformidad con el artículo 47;

e) no se ha efectuado el registro en la base de datos de la UE de conformidad con el artículo 71;

f) cuando proceda, no se ha designado a un representante autorizado;

g) no se dispone de documentación técnica.

2. Si el incumplimiento a que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado del Estado miembro de que se trate adoptará medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para asegurarse de que se recupera o retira del mercado sin demora.

Artículo 84
Estructuras de apoyo a los ensayos de IA de la Unión

1. La Comisión designará una o varias estructuras de apoyo a los ensayos de IA de la Unión para realizar las actividades enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 2019/1020 en el ámbito de la IA.

2. Sin perjuicio de las actividades a que se refiere el apartado 1, las estructuras de apoyo a los ensayos de IA de la Unión también proporcionarán asesoramiento técnico o científico independiente a petición del Consejo de IA, la Comisión o de las autoridades de vigilancia del mercado.

SECCIÓN 4
Vías de recurso

Artículo 85
Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado

Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en

el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente.

De conformidad con el Reglamento (UE) 2019/1020, tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos con este fin por las autoridades de vigilancia del mercado.

Artículo 86
Derecho a explicación de decisiones tomadas individualmente

1. Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

2. No se aplicará el apartado 1 a la utilización de sistemas de IA para los que existan excepciones o restricciones a la obligación prevista en dicho apartado derivadas del Derecho de la Unión o nacional de conformidad con el Derecho de la Unión.

3. El presente artículo se aplicará únicamente en la medida en que el derecho a que se refiere el apartado 1 no esté previsto de otro modo en el Derecho de la Unión.

Artículo 87
Denuncia de infracciones y protección de los denunciantes

La Directiva (UE) 2019/1937 se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien tales infracciones.

SECCIÓN 5
Supervisión, investigación, cumplimiento y seguimiento respecto de proveedores de modelos de IA de uso general

Artículo 88
Cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general

1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo V, teniendo en cuenta las garantías procedimentales previstas en el artículo 94. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de

las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados.

2. Sin perjuicio de lo dispuesto en el artículo 75, apartado 3, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las facultades previstas en la presente sección, cuando resulte necesario y proporcionado para ayudar a que se lleven a cabo las actividades de su competencia en virtud del presente Reglamento.

Artículo 89
Medidas de seguimiento

1. Con el fin de llevar a cabo los cometidos que se le atribuyen en la presente sección, la Oficina de IA podrá tomar las medidas necesarias para supervisar la aplicación y cumplimiento efectivos del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida su observancia de los códigos de buenas prácticas aprobados.

2. Los proveedores posteriores tendrán derecho a presentar reclamaciones alegando infracciones del presente Reglamento. Las reclamaciones deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general de que se trate;

b) una descripción de los hechos, las disposiciones del presente Reglamento afectadas y los motivos por los que el proveedor posterior considera que el proveedor del modelo de IA de uso general de que se trate ha infringido el presente Reglamento;

c) cualquier otra información que el proveedor posterior que presente la reclamación considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

Artículo 90
Alertas del grupo de expertos científicos sobre riesgos sistémicos

1. El grupo de expertos científicos podrá proporcionar alertas cualificadas a la Oficina de IA cuando tenga motivos para sospechar que:

a) un modelo de IA de uso general plantea un riesgo concreto reconocible a escala de la Unión, o

b) un modelo de IA de uso general reúne las condiciones a que se refiere el artículo 51.

2. Tras recibir dicha alerta cualificada, la Comisión podrá ejercer, a través de la Oficina de IA y tras haber informado al Consejo de IA, las facultades previstas en la presente sección con el fin de evaluar la cuestión. La Oficina de IA informará al Consejo de IA de cualquier medida que se adopte de conformidad con los artículos 91 a 94.

3. Las alertas cualificadas deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general con riesgo sistémico de que se trate;

b) una descripción de los hechos y los motivos por los que el grupo de expertos científicos proporciona la alerta;

c) cualquier otra información que el grupo de expertos científicos considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

Artículo 91
Poderes para solicitar documentación e información

1. La Comisión podrá solicitar al proveedor del modelo de IA de uso general interesado que facilite la documentación preparada por el proveedor de conformidad con los artículos 53 y 55, o cualquier otra información que sea necesaria para evaluar el cumplimiento del presente Reglamento por parte del proveedor.

2. Antes de enviar la solicitud de información, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Cuando el grupo de expertos científicos presente la correspondiente solicitud debidamente motivada, la Comisión podrá dirigir al proveedor de un modelo de IA de uso general una solicitud de información si el acceso a dicha información resulta necesario y proporcionado para que el grupo de expertos científicos pueda llevar a cabo sus cometidos en virtud del artículo 68, apartado 2.

4. La solicitud de información indicará la base jurídica y la finalidad de la solicitud, precisará qué información se requiere, fijará el plazo en el que deberá facilitarse la información e indicará las multas que se establecen en el artículo 101 por facilitar información incorrecta, incompleta o engañosa.

5. El proveedor del modelo de IA de uso general interesado, o su representante, facilitará la información solicitada. De tratarse de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas facilitarán la información solicitada en nombre del proveedor del modelo de IA de uso general interesado. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. Los representados seguirán siendo, no obstante, plenamente responsables, si la información facilitada es incompleta, incorrecta o engañosa.

Artículo 92
Poderes para realizar evaluaciones

1. La Oficina de IA, previa consulta al Consejo de IA, podrá realizar evaluaciones del modelo de IA de uso general de que se trate con el fin de:

a) evaluar si el proveedor cumple sus obligaciones en virtud del presente Reglamento, cuando la información recabada con arreglo al artículo 91 resulte insuficiente, o

b) investigar riesgos sistémicos a escala de la Unión de modelos de IA de uso general con riesgo sistémico, en particular a raíz de una alerta cualificada del grupo de expertos científicos de conformidad con el artículo 90, apartado 1, letra a).

2. La Comisión podrá decidir nombrar a expertos independientes para que realicen las evaluaciones en su nombre, también expertos científicos del grupo establecido de conformidad con el artículo 68. Los expertos independientes que se nombren para realizar estas tareas cumplirán los criterios establecidos en el artículo 68, apartado 2.

3. A los efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de uso general de que se trate a través de API o de otros medios y herramientas técnicos adecuados, como, por ejemplo, el código fuente.

4. La solicitud de acceso indicará la base jurídica, la finalidad y los motivos de la solicitud, y fijará el plazo durante el que deberá facilitarse el acceso y las multas que se establecen en el artículo 101 por no facilitarlo.

5. Los proveedores del modelo de IA de uso general interesados o su representante facilitarán la información solicitada. En caso de que se trate de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA de uso general interesado.

6. La Comisión adoptará actos de ejecución en los que se establezcan las modalidades detalladas y las condiciones de las evaluaciones, incluidas las disposiciones detalladas para la participación de expertos independientes y el procedimiento para su selección. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

7. Antes de solicitar el acceso al modelo de IA de uso general de que se trate, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general para recabar más información sobre los ensayos internos del modelo, las salvaguardias internas para prevenir los riesgos sistémicos y otros procedimientos y medidas internos que el proveedor haya adoptado para mitigar tales riesgos.

Artículo 93

Poderes para solicitar la adopción de medidas

1. Cuando resulte necesario y conveniente, la Comisión podrá solicitar a los proveedores que:

a) adopten las medidas oportunas para cumplir las obligaciones establecidas en los artículos 53 y 54;

b) apliquen medidas de reducción de riesgos cuando la evaluación realizada de conformidad con el artículo 92 apunte a que existen motivos serios y fundados de preocupación por la existencia de un riesgo sistémico a escala de la Unión;

c) restrinjan la comercialización del modelo, lo retiren o lo recuperen.

2. Antes de solicitar que se adopten medidas, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Si, durante el diálogo estructurado a que se refiere el apartado 2, el proveedor del modelo de IA de uso general con riesgo sistémico se compromete a adoptar medidas de reducción para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante una decisión, hacer dichos compromisos vinculantes y declarar que no hay ya motivos para actuar.

Artículo 94

Garantías procesales de los operadores económicos del modelo de IA de uso general

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará *mutatis mutandis* a los proveedores del modelo de IA de uso general, sin perjuicio de las garantías procesales más específicas previstas en el presente Reglamento.

CAPÍTULO X
CÓDIGOS DE CONDUCTA Y DIRECTRICES

Artículo 95

Códigos de conducta para la aplicación voluntaria de requisitos específicos

1. La Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, con los correspondientes mecanismos de gobernanza, destinados a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2, a los sistemas de IA que no sean de alto riesgo, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos.

2. La Oficina de IA y los Estados miembros facilitarán la elaboración de códigos de conducta relativos a la aplicación voluntaria, también por parte de los responsables del despliegue, de requisitos específicos para todos los sistemas de IA, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos, incluidos, entre otros pero no exclusivamente, elementos como:

a) los elementos aplicables establecidos en las Directrices éticas de la Unión para una IA fiable;

b) la evaluación y reducción al mínimo de las repercusiones de los sistemas de IA en la sostenibilidad medioambiental, también por cuanto se refiere a la programación eficiente desde el punto de vista energético y las técnicas para diseñar, entrenar y utilizar la IA de manera eficiente;

c) la promoción de la alfabetización en materia de IA, en particular en el caso de las personas que se ocupan del desarrollo, funcionamiento y utilización de la IA;

d) la facilitación de un diseño inclusivo y diverso de los sistemas de IA, por ejemplo mediante la creación de equipos de desarrollo inclusivos y diversos y la promoción de la participación de las partes interesadas en dicho proceso;

e) la evaluación y prevención de los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables, también por cuanto se refiere a accesibilidad para las personas con discapacidad, así como para la igualdad de género.

3. Los códigos de conducta podrán ser elaborados por proveedores o responsables del despliegue de sistemas de IA particulares, por las organizaciones que los representen o por ambos, también con la participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta podrán comprender uno o varios sistemas de IA en función de la similitud de la finalidad prevista de los distintos sistemas.

4. La Oficina de IA y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las pymes, incluidas las empresas emergentes, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

Artículo 96

Directrices de la Comisión sobre la aplicación del presente Reglamento

1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:

a) la aplicación de los requisitos y obligaciones a que se refieren los artículos 8 a 15 y el artículo 25;

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

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

d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50;

e) información detallada sobre la relación entre el presente Reglamento y la lista de actos legislativos de armonización de la Unión enumerados en el anexo I, así como otras disposiciones de Derecho de la Unión pertinentes, también por cuanto se refiere a la coherencia en su aplicación;

f) la aplicación de la definición de sistema de IA que figura en el artículo 3, punto 1.

Al publicar estas directrices, la Comisión prestará especial atención a las necesidades de las pymes, incluidas las empresas emergentes, de las autoridades públicas locales y de los sectores que tengan más probabilidades de verse afectados por el presente Reglamento.

Las directrices a que se refiere el párrafo primero del presente apartado tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas que se establezcan con arreglo al Derecho de armonización de la Unión.

2. A petición de los Estados miembros o de la Oficina de IA, o por propia iniciativa, la Comisión actualizará las directrices anteriormente adoptadas cuando se considere necesario.

CAPÍTULO XI
DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

Artículo 97
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. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, se otorgan a la Comisión por un período de cinco años a partir del 1 de agosto de 2024. 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 mencionada en el artículo 6, apartados 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 6, apartados 6 o 7, el artículo 7, apartados 1 o 3, el artículo 11, apartado 3, el artículo 43, apartados 5 o 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, o el artículo 53, apartados 5 o 6, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 98
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, se aplicará el artículo 5 del Reglamento (UE) n.o 182/2011.

CAPÍTULO XII
SANCIONES

Artículo 99
Sanciones

1. De conformidad con las condiciones previstas en el presente Reglamento, los Estados miembros establecerán el régimen de sanciones y otras medidas de ejecución, como advertencias o medidas no pecuniarias, aplicable a las infracciones del presente Reglamento que cometan los operadores y adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva y teniendo así en cuenta las directrices emitidas por la Comisión con arreglo al artículo 96. Tales sanciones serán efectivas, proporcionadas y disuasorias. Tendrán en cuenta los intereses de las pymes, incluidas las empresas emergentes, así como su viabilidad económica.

2. Los Estados miembros comunicarán a la Comisión, sin demora y, como muy tarde, en la fecha de aplicación las normas referentes a las sanciones y otras medidas de ejecución mencionadas en el apartado 1 y la informará, sin demora, de toda modificación de dichas normas.

3. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

4. El incumplimiento de cualquiera de las disposiciones que figuran a continuación en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5, estará sujeto a multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior:

a) las obligaciones de los proveedores con arreglo al artículo 16;

b) las obligaciones de los representantes autorizados con arreglo al artículo 22;

c) las obligaciones de los importadores con arreglo al artículo 23;

d) las obligaciones de los distribuidores con arreglo al artículo 24;

e) las obligaciones de los responsables del despliegue con arreglo al artículo 26;

f) los requisitos y obligaciones de los organismos notificados con arreglo al artículo 31, al artículo 33, apartados 1, 3 y 4, o al artículo 34;

g) las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50.

5. La presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

6. En el caso de las pymes, incluidas las empresas emergentes, cada una de las multas a que se refiere el presente artículo podrá ser por el porcentaje o el importe a que se refieren los apartados 3, 4 y 5, según cuál de ellos sea menor.

7. 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, en su caso, se tendrá en cuenta lo siguiente:

a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA y, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

b) si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por la misma infracción;

c) si otras autoridades han impuesto ya multas administrativas al mismo operador por infracciones de otros actos legislativos nacionales o de la Unión, cuando dichas infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;

d) el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción;

e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción;

f) el grado de cooperación con las autoridades nacionales competentes con el fin de subsanar la infracción y mitigar sus posibles efectos adversos;

g) el grado de responsabilidad del operador, teniendo en cuenta las medidas técnicas y organizativas aplicadas por este;

h) la forma en que las autoridades nacionales competentes tuvieron conocimiento de la infracción, en particular si el operador notificó la infracción y, en tal caso, en qué medida;

i) la intencionalidad o negligencia en la infracción;

j) las acciones emprendidas por el operador para mitigar los perjuicios sufridos por las personas afectadas.

8. Cada Estado miembro establecerá normas que determinen en qué medida es posible imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

9. 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.

10. El ejercicio de poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y nacional, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

11. Los Estados miembros informarán anualmente a la Comisión de las multas administrativas que hayan impuesto durante ese año de conformidad con el presente artículo y de cualquier litigio o proceso judicial relacionados.

Artículo 100

Multas administrativas a instituciones, órganos y organismos de la Unión

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, órganos y organismos de la Unión 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, teniendo en cuenta la finalidad del sistema de IA de que se trate, así como, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

b) el grado de responsabilidad de la institución, órgano u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas;

c) las acciones emprendidas por la institución, órgano u organismo de la Unión para mitigar los perjuicios sufridos por las personas afectadas;

d) el grado de cooperación con el Supervisor Europeo de Protección de Datos con el fin de subsanar 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, órgano u organismo de la Unión de que se trate en relación con el mismo asunto;

e) toda infracción anterior similar cometida por la institución, órgano u organismo de la Unión;

f) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución, órgano u organismo de la Unión notificó la infracción y, en tal caso, en qué medida;

g) el presupuesto anual de la institución, órgano u organismo de la Unión.

2. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 1 500 000 EUR.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento, distintos de los previstos en el artículo 5, estará sujeto a multas administrativas de hasta 750 000 EUR.

4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, órgano 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 los que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, participarán estrechamente en el 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 contribuirá al presupuesto general de la Unión. Las multas no afectarán al funcionamiento efectivo de la institución, órgano u organismo de la Unión sancionado.

7. El Supervisor Europeo de Protección de Datos informará anualmente a la Comisión de las multas administrativas que haya impuesto en virtud del presente artículo y de cualquier litigio o proceso judicial que haya iniciado.

Artículo 101
Multas a proveedores de modelos de IA de uso general

1. La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 000 000 EUR, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia:

a) infringieron las disposiciones pertinentes del presente Reglamento;

b) no atendieron una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta o engañosa;

c) incumplieron una medida solicitada en virtud del artículo 93;

d) no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

Al fijar el importe de la multa o de la multa coercitiva, se tomarán en consideración la naturaleza, gravedad y duración de la infracción, teniendo debidamente en cuenta los

principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el artículo 93, apartado 3, y en los códigos de buenas prácticas pertinentes previstos en el artículo 56.

2. Antes de adoptar una decisión con arreglo al apartado 1, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de uso general o del modelo de IA y le dará la oportunidad de ser oído.

3. Las multas impuestas de conformidad con el presente artículo serán efectivas, proporcionadas y disuasorias.

4. La información sobre las multas impuestas en virtud del presente artículo también se comunicará al Consejo de IA, según proceda.

5. El Tribunal de Justicia de la Unión Europea tendrá plena competencia jurisdiccional para examinar las decisiones de imposición de una multa adoptadas por la Comisión en virtud del presente artículo. Podrá anular, reducir o incrementar la cuantía de la multa impuesta.

6. La Comisión adoptará actos de ejecución que contengan disposiciones detalladas y garantías procesales para los procedimientos con vistas a la posible adopción de decisiones con arreglo al apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO XIII
DISPOSICIONES FINALES

Artículo 102
Modificación del Reglamento (CE) 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) 2024/1689 del Parlamento Europeo y del Consejo[2], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

---

2 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)

Artículo 103
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) 2024/1689 del Parlamento Europeo y del Consejo[3], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 104
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) 2024/1689 del Parlamento Europeo y del Consejo[4], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 105
Modificación de la Directiva 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

> «5. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento

---

3 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

4 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Europeo y del Consejo[5], la Comisión tendrá en cuenta los requisitos establecidos en el capítulo III, sección 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.

Artículo 106
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) 2024/1689 del Parlamento Europeo y del Consejo[6], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 107
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) 2024/… del Parlamento Europeo y del Consejo[7], se

---

5 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

6 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

7 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y

tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 108
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) 2024/1689 del Parlamento Europeo y del Consejo[8], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

8 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

5) En el artículo 57, se añade el párrafo siguiente:

> Al adoptar dichos actos de ejecución relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 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 sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 109
Modificación del Reglamento (UE) 2019/2144

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el párrafo siguiente:

> 3. Al adoptar actos de ejecución en virtud del apartado 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo[9], se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 110
Modificación de la Directiva (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo [10] se añade el punto siguiente:

> 68) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 1689, por el que se establecen normas armonizadas en materia de inteligencia

---

9 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

10 Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Artículo 111

Sistemas de IA ya introducidos en el mercado o puestos en servicio y modelos de IA de uso general ya introducidos en el mercado

1. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo X que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2027 deberán estar en conformidad con el presente Reglamento a más tardar el 31 de diciembre de 2030.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta en la evaluación de cada sistema informático de gran magnitud establecido en virtud de los actos jurídicos enumerados en el anexo X que se efectúe de conformidad con lo dispuesto en dichos actos jurídicos y cuando dichos actos jurídicos hayan sido sustituidos o modificados.

2. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), el presente Reglamento se aplicará a los operadores de sistemas de IA de alto riesgo, distintos de los mencionados en el apartado 1 del presente artículo, que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2026 únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en su diseño. En cualquier caso, los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas adoptarán las medidas necesarias para cumplir los requisitos y obligaciones del presente Reglamento a más tardar el 2 de agosto de 2030.

3. Los proveedores de modelos de IA de uso general que se hayan introducido en el mercado antes del 2 de agosto de 2025 adoptarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el 2 de agosto de 2027.

Artículo 112

Evaluación y revisión

1. La Comisión evaluará la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5 una vez al año a partir de la entrada en vigor del presente Reglamento y hasta el final del período de delegación de poderes previsto en el artículo 97. La Comisión presentará las conclusiones de dicha evaluación al Parlamento Europeo y al Consejo.

2. A más tardar el 2 de agosto de 2028, y posteriormente cada cuatro años, la Comisión evaluará los puntos siguientes e informará de ello al Parlamento Europeo y al Consejo:

a) la necesidad de ampliar los ámbitos enumerados en el anexo III o de añadir nuevos ámbitos;

b) la necesidad de modificar la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50;

c) la necesidad de mejorar la eficacia del sistema de supervisión y gobernanza.

3. A más tardar el 2 de agosto de 2029, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. El informe incluirá una evaluación de la estructura de control del cumplimiento y de la posible necesidad de que una agencia de la Unión resuelva las deficiencias detectadas. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento. Los informes se harán públicos.

4. En los informes mencionados en el apartado 2 se prestará una atención especial a lo siguiente:

a) el estado de los recursos financieros, técnicos y humanos de las autoridades nacionales competentes para desempeñar de forma eficaz las funciones que les hayan sido asignadas en virtud del presente Reglamento;

b) el estado de las sanciones, en particular, de las multas administrativas a que se refiere el artículo 99, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento;

c) las normas armonizadas adoptadas y las especificaciones comunes desarrolladas en apoyo del presente Reglamento;

d) el número de empresas que entran en el mercado después de que se empiece a aplicar el presente Reglamento y, de entre ellas, el número de pymes.

5. A más tardar el 2 de agosto de 2028, la Comisión evaluará el funcionamiento de la Oficina de IA, si se le han otorgado poderes y competencias suficientes para desempeñar sus funciones, y si sería pertinente y necesario para la correcta aplicación y ejecución del presente Reglamento mejorar la Oficina de IA y sus competencias de ejecución, así como aumentar sus recursos. La Comisión presentará un informe sobre su evaluación al Parlamento Europeo y al Consejo.

6. A más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión presentará un informe sobre la revisión de los avances en la elaboración de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general y evaluará la necesidad de medidas o acciones adicionales, incluidas medidas o acciones vinculantes. Este informe se remitirá al Parlamento Europeo y al Consejo y se hará público.

7. A más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión evaluará la incidencia y la eficacia de los códigos de conducta voluntarios por lo que respecta a promover la aplicación de los requisitos establecidos en el capítulo III, sección 2, a sistemas de IA que no sean de alto riesgo y, en su caso, de otros requisitos adicionales aplicables a los sistemas de IA que no sean sistemas de IA de alto riesgo, como, por ejemplo, requisitos relativos a la sostenibilidad medioambiental.

8. A efectos de lo dispuesto en los apartados 1 a 7, el Consejo de IA, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión, cuando así lo solicite, y sin demora indebida.

9. Al llevar a cabo las evaluaciones y revisiones mencionadas en los apartados 1 a 7, la Comisión tendrá en cuenta las posiciones y conclusiones del Consejo de IA, el Parlamento Europeo, el Consejo y los demás organismos o fuentes pertinentes.

10. 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 el efecto de los sistemas de IA en la salud y la seguridad y en los derechos fundamentales, y a la vista de los avances en la sociedad de la información.

11. Para orientar las evaluaciones y revisiones a que se refieren los apartados 1 a 7 del presente artículo, la Oficina de IA se encargará de desarrollar una metodología objetiva y participativa para la evaluación de los niveles de riesgo a partir de los criterios expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en:

a) la lista establecida en el anexo III, incluida la ampliación de los ámbitos existentes o la inclusión de nuevos ámbitos en dicho anexo;

b) la lista de prácticas prohibidas establecida en el artículo 5, y

c) la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50.

12. Las modificaciones del presente Reglamento con arreglo al apartado 10, o los actos delegados o de ejecución pertinentes, que afecten a los actos legislativos de armonización de la Unión sectoriales que se enumeran en el anexo I, sección B, tendrán en cuenta las particularidades normativas de cada sector y los mecanismos de gobernanza, evaluación de la conformidad y ejecución vigentes, así como las autoridades establecidas en ellos.

13. A más tardar el 2 de agosto de 2031, la Comisión evaluará la ejecución del presente Reglamento e informará al respecto al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del presente Reglamento. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que respecta a la estructura de ejecución y a la necesidad de que una agencia de la Unión resuelva las deficiencias detectadas.

Artículo 113

Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*. Será aplicable a partir del 2 de agosto de 2026.

No obstante:

a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;

b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;

c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 13 de junio de 2024.

Por el Parlamento Europeo
La Presidenta
R. METSOLA

Por el Consejo El Presidente
M. MICHEL