UNIÓN EUROPEA

EL PARLAMENTO EUROPEO **EL CONSEJO**

Bruselas, 25 de septiembre de 2024
(OR. en)

2022/0272(COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

ACTOS LEGISLATIVOS Y OTROS INSTRUMENTOS

Asunto:	REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia)

REGLAMENTO (UE) 2024/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de …

relativo a los requisitos horizontales de ciberseguridad
para los productos con elementos digitales
y por el que se modifica el Reglamento (UE) n.º 168/2013
y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828
(Reglamento de Ciberresiliencia)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité Económico y Social Europeo[1],

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario[2],

---

1 DO C 100 de 16.3.2023, p. 101.
2 Posición del Parlamento Europeo de 12 de marzo de 2024 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de ….

Considerando lo siguiente:

(1) La ciberseguridad es uno de los principales retos para la Unión. El número y la variedad de dispositivos conectados aumentará exponencialmente en los próximos años. Los ciberataques constituyen un asunto de interés público, ya que tienen un impacto crítico no solo en la economía de la Unión, sino también en la democracia y en la salud y la seguridad de los consumidores. Por lo tanto, es necesario reforzar el enfoque de la Unión respecto a la ciberseguridad, abordar la ciberresiliencia a escala de la Unión y mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la introducción de productos con elementos digitales en el mercado la Unión. Deben abordarse dos problemas importantes que suponen un aumento de los costes para los usuarios y la sociedad: un bajo nivel de ciberseguridad de los productos con elementos digitales, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y la insuficiencia de la comprensión de la información y del acceso a ella por parte de los usuarios, que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

(2) El presente Reglamento tiene por objeto fijar condiciones límite que permitan el desarrollo de productos con elementos digitales seguros, garantizando que los productos consistentes en equipos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto. También aspira a crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utilizar productos con elementos digitales, por ejemplo, mejorando la transparencia con respecto al período de soporte de los productos con elementos digitales comercializados.

(3) El Derecho pertinente de la Unión en vigor está compuesto por varios conjuntos de normas horizontales que abordan determinados aspectos relacionados con la ciberseguridad desde diferentes perspectivas, incluidas medidas para mejorar la seguridad de la cadena de suministro digital. Sin embargo, el Derecho vigente de la Unión relativo a la ciberseguridad, incluidos el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[3] y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[4], no aborda de manera directa los requisitos obligatorios para la seguridad de los productos con elementos digitales.

---

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

[4] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

(4) Aunque el Derecho vigente de la Unión se aplica a determinados productos con elementos digitales, no existe un marco regulador horizontal de la Unión que establezca requisitos de ciberseguridad exhaustivos para todos los productos con elementos digitales. Los diversos actos e iniciativas adoptados hasta la fecha a escala nacional y de la Unión abordan solo de manera parcial los problemas y riesgos detectados en relación con la ciberseguridad, creando un mosaico legislativo dentro del mercado interior, aumentando la inseguridad jurídica tanto para los fabricantes como para los usuarios de dichos productos y añadiendo una carga innecesaria a las empresas y las organizaciones vinculadas al cumplimiento de una serie de requisitos y obligaciones para tipos de productos similares. La ciberseguridad de esos productos tiene una dimensión transfronteriza de particular importancia, ya que los productos con elementos digitales fabricados en un Estado miembro o en un país tercero suelen ser utilizados por organizaciones y consumidores en todo el mercado interior. Por todo ello se hace necesario regular este ámbito a escala de la Unión para garantizar un marco regulador armonizado y la seguridad jurídica para los usuarios, las organizaciones y las empresas, incluidas las microempresas y las pequeñas y medianas empresas, tal como se definen en el anexo de la Recomendación 2003/361/CE de la Comisión[5]. El panorama normativo de la Unión debe armonizarse mediante la introducción de requisitos horizontales de ciberseguridad para los productos con elementos digitales. Además, debe garantizarse en toda la Unión una mayor seguridad jurídica para los operadores económicos y los usuarios, así como una mejor armonización del mercado interior, de una forma proporcional para las microempresas y las pequeñas y medianas empresas, y de este modo establecer condiciones más viables para los operadores económicos que deseen acceder a dicho mercado.

[5] Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

(5) Por lo que se refiere a las microempresas y a las pequeñas y medianas empresas, a la hora de determinar la categoría a la que pertenece una empresa, deben aplicarse en su totalidad las disposiciones del anexo de la Recomendación 2003/361/CE. Por lo tanto, al calcular los efectivos y los límites financieros que determinan las categorías de empresas, también deben aplicarse las disposiciones del artículo 6 del anexo de la Recomendación 2003/361/CE, sobre la determinación de los datos de una empresa, como las empresas asociadas o las empresas vinculadas.

(6) La Comisión debe proporcionar orientaciones para ayudar a los operadores económicos, en particular a las microempresas y a las pequeñas y medianas empresas, en la aplicación del presente Reglamento. Esas orientaciones deben abarcar, entre otros aspectos, el ámbito de aplicación del presente Reglamento, en particular el tratamiento de datos a distancia y sus implicaciones para los desarrolladores de programas informáticos libres y de código abierto, la aplicación de los criterios utilizados para determinar los períodos de soporte de los productos con elementos digitales, la interacción entre el presente Reglamento y el resto del Derecho de la Unión y el concepto de modificación sustancial.

(7) A escala de la Unión, diversos documentos programáticos y políticos, como la Comunicación conjunta de la Comisión y del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 16 de diciembre de 2020, titulada «Estrategia de Ciberseguridad de la UE para la Década Digital», las Conclusiones del Consejo, de 2 de diciembre de 2020, sobre la ciberseguridad de los dispositivos conectados, y de 23 de mayo de 2022, sobre el desarrollo de la posición de la Unión Europea en materia de ciberseguridad y la Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital[6], han hecho un llamamiento a que se establezcan requisitos específicos de ciberseguridad de la Unión para los productos digitales o conectados, y varios terceros países han introducido por iniciativa propia medidas para abordar esta cuestión. En el informe final de la Conferencia sobre el Futuro de Europa, los ciudadanos pidieron «reforzar el papel de la Unión en la lucha contra las amenazas a la ciberseguridad». A fin de que la Unión desempeñe internacionalmente un papel protagonista en materia de ciberseguridad, es importante establecer un marco normativo general ambicioso.

(8) Para aumentar el nivel general de ciberseguridad de todos los productos con elementos digitales que se comercialicen en el mercado interior, es necesario disponer de requisitos esenciales de ciberseguridad orientados a objetivos y tecnológicamente neutros que se apliquen horizontalmente a esos productos.

---

[6] DO C 67 de 8.2.2022, p. 81.

(9) En determinadas condiciones, todos los productos con elementos digitales integrados en un sistema electrónico de información más amplio o conectados a este pueden servir de vector de ataque para agentes malintencionados. En consecuencia, incluso los equipos y programas informáticos considerados menos críticos pueden facilitar que un dispositivo o red se vea comprometido en una fase inicial, lo que permite a los agentes malintencionados obtener un acceso privilegiado a un sistema o moverse lateralmente entre sistemas. Por consiguiente, los fabricantes deben garantizar que todos los productos con elementos digitales se diseñen y desarrollen de conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. Esta obligación se refiere tanto los productos que puedan conectarse físicamente, a través de interfaces en los equipos informáticos, como los que se conecten mediante conexiones lógicas, a través, por ejemplo, de zócalos, conductos, archivos, interfaces de programación de aplicaciones o cualquier otro tipo de interfaz de programa. Teniendo en cuenta que las amenazas a la ciberseguridad pueden propagarse a través de diversos productos con elementos digitales antes de alcanzar un objetivo determinado, por ejemplo, mediante el aprovechamiento sucesivo de múltiples vulnerabilidades, los fabricantes también deben garantizar la ciberseguridad de los productos cuya conexión a otros dispositivos o redes es indirecta.

(10) El establecimiento de requisitos de ciberseguridad para la introducción en el mercado de productos con elementos digitales persigue la mejora de la ciberseguridad de dichos productos tanto para los consumidores como para las empresas. Esos requisitos garantizarán asimismo que se tenga en cuenta la ciberseguridad a lo largo de todas las cadenas de suministro, mejorando así la seguridad de los productos finales con elementos digitales. Entre ellos se incluyen requisitos para la introducción en el mercado de productos de consumo con elementos digitales destinados a consumidores vulnerables, como juguetes y sistemas de vigilancia de bebés. Los productos de consumo con elementos digitales clasificados en el presente Reglamento como productos importantes con elementos digitales presentan un mayor riesgo de ciberseguridad al desempeñar una función que conlleva un riesgo significativo de efectos adversos en términos de intensidad y capacidad para dañar la salud, la protección o la seguridad de los usuarios de dichos productos, y deben someterse a un procedimiento de evaluación de la conformidad más estricto. Ello se aplica a productos como los domésticos inteligentes con funcionalidades de seguridad, incluidas las cerraduras inteligentes de puertas, los sistemas de vigilancia de bebés y los sistemas de alarma, los juguetes conectados y las tecnologías sanitarias personales ponibles. Además, los procedimientos de evaluación de la conformidad más estrictos que deben someterse otros productos con elementos digitales clasificados en el presente Reglamento como productos importantes o críticos con elementos digitales contribuirán a prevenir los posibles efectos negativos de la explotación de las vulnerabilidades para los consumidores.

(11) El presente Reglamento tiene por objeto garantizar un elevado nivel de ciberseguridad en productos con elementos digitales y sus soluciones de tratamiento de datos a distancia integradas. Tales soluciones de tratamiento de datos deben definirse como todo tratamiento de datos a distancia para el que el programa informático haya sido diseñado y desarrollado por el fabricante del producto con elementos digitales en cuestión o en su nombre, y cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones. Este enfoque garantiza que esos productos estén adecuadamente protegidos en su totalidad por sus fabricantes, con independencia de que los datos sean tratados o almacenados localmente en el dispositivo del usuario o a distancia por el fabricante. Al mismo tiempo, el tratamiento o el almacenamiento a distancia entran en el ámbito de aplicación del presente Reglamento únicamente en la medida en que sea necesario para que un producto con elementos digitales desempeñe sus funciones. Este tratamiento o almacenamiento a distancia incluye la situación en la que una aplicación móvil requiere el acceso a una interfaz de programación de aplicaciones o a una base de datos facilitada por medio de un servicio desarrollado por el fabricante. En tal caso, el servicio entra en el ámbito de aplicación del presente Reglamento como solución de tratamiento de datos a distancia. Los requisitos relativos a las soluciones de tratamiento de datos a distancia que entran en el ámbito de aplicación del presente Reglamento no implican, por tanto, medidas técnicas, operativas u organizativas destinadas a gestionar los riesgos para la seguridad de las redes y los sistemas de información de un fabricante en su conjunto.

(12) Las soluciones en la nube solo constituyen soluciones de tratamiento de datos a distancia en el sentido del presente Reglamento si se ajustan a la definición establecida en el presente Reglamento. Por ejemplo, las funciones habilitadas en la nube y prestadas por el fabricante de dispositivos para el hogar inteligente que permiten a los usuarios controlar el dispositivo de que se trate a distancia, entran en el ámbito de aplicación del presente Reglamento. Por otra parte, los sitios web que no admiten la funcionalidad de un producto con elementos digitales o los servicios en la nube diseñados y desarrollados fuera de la responsabilidad de un fabricante de un producto con elementos digitales no entran en el ámbito de aplicación del presente Reglamento. La Directiva (UE) 2022/2555 se aplica a los servicios de computación en la nube y a los modelos de servicios en nube, como la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS), el software como servicio (SaaS) y la red como servicio (NaaS). Las entidades que presten servicios de computación en la nube en la Unión que se consideren medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE, o que superen los límites máximos para las medianas empresas previstos en el apartado 1 de ese artículo, entran en el ámbito de aplicación de la Directiva.

(13) De acuerdo con el objetivo del presente Reglamento de eliminar las barreras a la libre circulación de los productos con elementos digitales, los Estados miembros no impedirán, para las cuestiones reguladas en el presente Reglamento, la comercialización de productos con elementos digitales que sean conformes con el presente Reglamento. Por consiguiente, para las cuestiones armonizadas por el presente Reglamento, los Estados miembros no pueden imponer requisitos de ciberseguridad adicionales para la comercialización de productos con elementos digitales. No obstante, cualquier entidad, pública o privada, puede establecer requisitos adicionales a los establecidos en el presente Reglamento para la contratación o el uso de productos con elementos digitales para sus fines específicos y, por tanto, puede optar por utilizar productos con elementos digitales que cumplan requisitos de ciberseguridad más estrictos o específicos que los aplicables para la comercialización en virtud del presente Reglamento. Sin perjuicio de lo dispuesto en las Directivas 2014/24/UE[7] y 2014/25/UE[8] del Parlamento Europeo y del Consejo, al adquirir productos con elementos digitales que deben cumplir los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, incluidos los relativos a la gestión de vulnerabilidades, los Estados miembros deben garantizar que esos requisitos se tengan en cuenta en el proceso de contratación pública y que también se tenga en cuenta la capacidad de los fabricantes para aplicar eficazmente las medidas de ciberseguridad y gestionar las ciberamenazas.

---

7 Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

8 Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE (DO L 94 de 28.3.2014, p. 243).

Además, la Directiva (UE) 2022/2555 establece medidas para la gestión de riesgos de ciberseguridad para las entidades esenciales e importantes a que se refiere el artículo 3 de dicha Directiva que podrían implicar medidas de seguridad de la cadena de suministro que exijan el uso por dichas entidades de productos con elementos digitales que cumplan requisitos de ciberseguridad más estrictos que los establecidos en el presente Reglamento. De conformidad con la Directiva (UE) 2022/2555 y en consonancia con su principio de armonización mínima, los Estados miembros pueden, por tanto, imponer requisitos de ciberseguridad adicionales para el uso de productos de TIC por parte de entidades esenciales o importantes en virtud de dicha Directiva, a fin de garantizar un mayor nivel de ciberseguridad, siempre que dichos requisitos sean coherentes con las obligaciones de los Estados miembros establecidas en el Derecho de la Unión. Las cuestiones no previstas en el presente Reglamento pueden incluir factores no técnicos relacionados con los productos con elementos digitales y sus fabricantes. Por consiguiente, los Estados miembros pueden establecer medidas nacionales, incluidas restricciones a los productos con elementos digitales o a los proveedores de esos productos que tengan en cuenta factores no técnicos. Las medidas nacionales relativas a tales factores deben ser conformes con el Derecho de la Unión.

(14) El presente Reglamento se entiende sin perjuicio de la responsabilidad de los Estados miembros para adoptar medidas que preserven la seguridad nacional, en cumplimiento del Derecho de la Unión. Los Estados miembros deben poder someter a medidas adicionales los productos con elementos digitales de los que hayan provisto, o que utilicen, con fines de seguridad nacional o defensa, siempre que dichas medidas sean coherentes con las obligaciones de los Estados miembros establecidas en el Derecho de la Unión.

(15) El presente Reglamento se aplica a los operadores económicos únicamente en relación con los productos con elementos digitales comercializados y, por tanto, suministrados para su distribución o uso en el mercado de la Unión en el transcurso de una actividad comercial. El suministro durante una actividad comercial puede caracterizarse no solo por la aplicación de un precio a un producto con elementos digitales, sino también por la aplicación de un precio a los servicios de asistencia técnica, cuando esta no se utilice únicamente para la recuperación de costes efectivos, mediante la intención de monetizar, por ejemplo por el suministro de una plataforma de software a través de la cual el fabricante monetiza otros servicios, requiriendo como condición para el uso el procesamiento de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático, o la aceptación de donaciones que excedan los costes asociados con el diseño, desarrollo y suministro de un producto con elementos digitales. La aceptación de donaciones sin la intención de obtener un beneficio no debe considerarse una actividad comercial.

(16) Los productos con elementos digitales proporcionados como parte de la prestación de un servicio por el que se cobra una tasa únicamente para recuperar los costes reales directamente relacionados con la explotación de dicho servicio, como puede ser el caso de determinados productos con elementos digitales proporcionados por entidades de la administración pública, no deben considerarse por esos mismos motivos una actividad comercial a efectos del presente Reglamento. Además, los productos con elementos digitales desarrollados o modificados por una entidad de la administración pública exclusivamente para su propio uso no deben considerarse comercializados en el sentido del presente Reglamento.

(17) Los programas informáticos y los datos que se compartan abiertamente y a los que los usuarios puedan acceder, usar, modificar y redistribuir con libertad (ya sean estos o versiones modificadas de ellos) pueden contribuir a la investigación e innovación en el mercado. Para promover el desarrollo y el despliegue de programas informáticos libres y de código abierto, en particular por parte de microempresas y pequeñas y medianas empresas, incluidas las empresas emergentes, los particulares y las organizaciones sin ánimo de lucro, y entidades y particulares dedicados a la investigación académica, la aplicación del presente Reglamento a los productos con elementos digitales considerados programas informáticos libres y de código abierto suministrados para la distribución o el uso durante una actividad comercial debe tener en cuenta la naturaleza de los diferentes modelos de desarrollo de programas informáticos distribuidos y desarrollados con arreglo programas informáticos libres y de código abierto.

(18) Un programa informático libre y de código abierto se entiende como un programa informático cuyo código fuente se comparte abiertamente y cuya licencia abarca todos los derechos para que el programa informático sea libremente accesible, utilizable, modificable y redistribuible. Los programas informáticos libres y de código abierto se desarrollan, mantienen y distribuyen abiertamente, también a través de plataformas en línea. En relación con los operadores económicos que entran en el ámbito de aplicación del presente Reglamento, solo deben entrar en el ámbito de aplicación del presente Reglamento los programas informáticos libres y de código abierto comercializados y, por tanto, suministrados para su distribución o uso en el transcurso de una actividad comercial. Por tanto, las circunstancias en las que el producto con elementos digitales se ha desarrollado el producto o el modo en que se ha financiado el desarrollo no se han de tener en cuenta a la hora de determinar el carácter comercial o no comercial de dicha actividad. Más concretamente, a efectos del presente Reglamento y en relación con los operadores económicos que entran en su ámbito de aplicación, a fin de garantizar que exista una distinción clara entre las fases de desarrollo y suministro, el suministro de productos con elementos digitales que se consideren programas informáticos libres y de código abierto que no sean monetizados por sus fabricantes no debe considerarse una actividad comercial. Además, el suministro de productos con elementos digitales que se consideren componentes de programas informáticos libres y de código abierto destinados a ser integrados por otros fabricantes en sus propios productos con elementos digitales no debe considerarse comercialización salvo que el componente sea monetizado por su fabricante original. Por ejemplo, el mero hecho de que un producto consistente en programas informáticos de código abierto con elementos digitales reciba apoyo financiero de los fabricantes o de que estos contribuyan al desarrollo de ese producto no debe determinar por sí solo que la actividad sea de carácter comercial.

Además, la mera presencia de liberaciones periódicas no debe llevar por sí misma a la conclusión de que un producto con elementos digitales se suministra en el transcurso de una actividad comercial. Por último, a efectos del presente Reglamento, el desarrollo de productos con elementos digitales que se consideren programas informáticos libres y de código abierto por parte de organizaciones sin ánimo de lucro no debe considerarse una actividad comercial, siempre que la organización se haya establecido de tal manera que se garantice que todos los ingresos después de los costes se utilicen para alcanzar objetivos sin ánimo de lucro. El presente Reglamento no se aplicará a las personas físicas o jurídicas que contribuyan con código fuente a productos con elementos digitales que se consideren programas informáticos libres y de código abierto que no estén bajo su responsabilidad.

(19) Teniendo en cuenta la importancia para la ciberseguridad de muchos productos con elementos digitales que se consideran programas informáticos libres y de código abierto que se publican, pero no se comercializan en el sentido del presente Reglamento, se debe aplicar a las personas jurídicas que prestan apoyo de forma sostenida para el desarrollo de esos productos destinados a actividades comerciales y que desempeñan un papel principal a la hora de garantizar la viabilidad de dichos productos (administradores de comunidad de programas informáticos de código abierto) un régimen regulador flexible y adaptado. Entre los administradores de comunidad programas informáticos de código abierto figuran determinadas fundaciones, así como entidades que desarrollan y publican programas informáticos libres y de código abierto en un contexto empresarial, incluidas las entidades sin ánimo de lucro. El régimen regulador debe tener en cuenta su naturaleza específica y su compatibilidad con el tipo de obligaciones impuestas. Solo debe abarcar los productos con elementos digitales calificados como programas informáticos libres y de código abierto que estén destinados en última instancia a actividades comerciales, como la integración en servicios comerciales o en productos monetizados con elementos digitales. A efectos de dicho régimen regulador, la intención de integración en productos monetizados con elementos digitales incluye los casos en que los fabricantes que integran un componente en sus propios productos con elementos digitales contribuyen al desarrollo de dicho componente de manera regular o prestan asistencia financiera periódica para garantizar la continuidad de un producto consistente en programas informáticos. La prestación de apoyo continuado al desarrollo de un producto con elementos digitales incluye, entre otras cosas, el alojamiento y la gestión de plataformas de colaboración para el desarrollo de programa informático, el alojamiento de códigos fuente o programas informáticos, la administración o gestión de productos con elementos digitales que se consideren programas informáticos libres y de código abierto, así como la dirección del desarrollo de dichos productos. Dado que el régimen regulador flexible y adaptado no somete a quienes intervienen en calidad de administradores de comunidad de programas informáticos de código abierto a las mismas obligaciones que quienes intervienen en calidad de fabricantes con arreglo al presente Reglamento, no debe permitirse que coloquen el marcado CE en los productos con elementos digitales cuyo desarrollo apoyan.

(20) El solo acto de albergar productos con elementos digitales en repositorios abiertos también a través de administradores de paquetes o en plataformas de colaboración no constituye en sí mismo una comercialización de un producto con elementos digitales. Los proveedores de esos servicios no deben ser considerados distribuidores salvo si comercializan esos programas informáticos y, por lo tanto, los suministran para su distribución o uso en el mercado de la Unión en el transcurso de una actividad comercial.

(21) Con el fin de apoyar y facilitar la diligencia debida de los fabricantes que integren componentes de programas informáticos libres y de código abierto que no estén sujetos a los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento en sus productos con elementos digitales, la Comisión debe poder establecer programas voluntarios de certificación de seguridad, bien mediante un acto delegado que complemente el presente Reglamento, bien solicitando un esquema europeo de certificación de la ciberseguridad con arreglo al artículo 48 del Reglamento (UE) 2019/881 que tenga en cuenta las especificidades de los modelos de desarrollo de programas informáticos libres y de código abierto. Los programas de verificación de seguridad deben concebirse de manera que no solo las personas físicas o jurídicas que desarrollen o contribuyan al desarrollo de un producto con elementos digitales que se consideren programas informáticos libres y de código abierto puedan iniciar o financiar una verificación de seguridad, sino también terceros, como los fabricantes que integren dichos productos en sus propios productos con elementos digitales, los usuarios o las administraciones públicas de la Unión y nacionales.

(22) En vista de los objetivos de ciberseguridad pública del presente Reglamento y con el fin de mejorar el conocimiento de la situación de los Estados miembros en lo que respecta a la dependencia de la Unión de los componentes consistentes en programas informáticos, en particular, de los componentes consistentes en programas informáticos potencialmente libres y de código abierto, un Grupo Específico de Cooperación Administrativa (ADCO, por sus siglas en inglés) establecido por el presente Reglamento debe poder decidir llevar a cabo conjuntamente una evaluación de la dependencia de la Unión. Las autoridades de vigilancia del mercado deben poder solicitar a los fabricantes de categorías de productos con elementos digitales establecidos por el ADCO que presenten las nomenclaturas de materiales de los programas informáticos (SBOM, por sus siglas en inglés) que hayan generado en virtud del presente Reglamento. Con el fin de proteger la confidencialidad de las SBOM, las autoridades de vigilancia del mercado deben presentar al ADCO la información pertinente sobre las dependencias de manera anonimizada y agregada.

(23) La eficacia de la aplicación del presente Reglamento dependerá también de la disponibilidad de capacidades adecuadas en materia de ciberseguridad. A escala de la Unión, varios documentos programáticos y políticos, incluida la Comunicación de la Comisión, de 18 de abril de 2023, titulada «Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE» y las Conclusiones del Consejo, de 22 de mayo de 2023, sobre la política de ciberdefensa de la UE, reconocieron el déficit de capacidades en materia de ciberseguridad en la Unión y la necesidad de abordar estos retos con carácter prioritario, tanto en el sector público como en el privado. Con el fin de garantizar una aplicación efectiva del presente Reglamento, los Estados miembros deben asegurarse de que se disponga de los recursos adecuados para que las autoridades de vigilancia del mercado y los organismos de evaluación de la conformidad cuenten con personal adecuado para llevar a cabo sus tareas tal como dispone el presente Reglamento. Estas medidas deben mejorar la movilidad de la mano de obra en el ámbito de la ciberseguridad y sus trayectorias profesionales asociadas. También deben contribuir a que la mano de obra en materia de ciberseguridad sea más resiliente e inclusiva, también en términos de género. Por consiguiente, los Estados miembros deben adoptar medidas para garantizar que dichas tareas las lleven a cabo profesionales adecuadamente formados, con las capacidades necesarias en materia de ciberseguridad. Del mismo modo, los fabricantes deben garantizar que su personal tenga las capacidades necesarias para cumplir sus obligaciones tal como dispone el presente Reglamento. Los Estados miembros y la Comisión, en consonancia con sus prerrogativas y competencias y con las tareas específicas que les confiere el presente Reglamento, deben adoptar medidas de apoyo a los fabricantes y, en particular, a las microempresas y a las pequeñas y medianas empresas, incluidas las empresas emergentes, también en ámbitos como el desarrollo de capacidades, a efectos del cumplimiento de sus obligaciones establecidas en el presente Reglamento. Además, dado que la Directiva (UE) 2022/2555 exige a los Estados miembros que adopten políticas que promuevan y desarrollen formación en materia de ciberseguridad y capacidades de ciberseguridad como parte de sus estrategias nacionales de ciberseguridad, al adoptar dichas estrategias los Estados miembros también pueden considerar que se aborden las necesidades en materia de capacidades de ciberseguridad derivadas del presente Reglamento, incluidas las relacionadas con el reciclaje profesional y el perfeccionamiento de las capacidades.

(24) Una internet segura es indispensable para el funcionamiento de las infraestructuras críticas y para la sociedad en su conjunto. La Directiva (UE) 2022/2555 tiene por objeto garantizar un elevado nivel de ciberseguridad de los servicios prestados por entidades esenciales e importantes mencionadas en el artículo 3 de la Directiva, incluidos los proveedores de infraestructuras digitales que apoyan las funciones básicas de la internet abierta o garantizan el acceso a internet y prestación de los servicios de internet. Por consiguiente, es importante que los productos con elementos digitales necesarios para que los proveedores de infraestructuras digitales garanticen el funcionamiento de internet se desarrollen de manera segura y cumplan normas de seguridad de internet bien establecidas. El presente Reglamento, que se aplica a todos los productos conectables consistentes en equipos y programas informáticos, tiene también por objeto facilitar que los proveedores de infraestructuras digitales cumplan los requisitos de la cadena de suministro con arreglo a la Directiva (UE) 2022/2555, garantizando que los productos con elementos digitales que utilizan para prestar sus servicios se desarrollen de forma segura y que tienen acceso a actualizaciones de seguridad oportunas para dichos productos.

(25) El Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo[9] establece normas sobre los productos sanitarios y el Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo[10] establece normas sobre los productos sanitarios para diagnóstico in vitro. Esos Reglamentos abordan los riesgos de ciberseguridad y adoptan enfoques particulares que el presente Reglamento también aborda. Más concretamente, los Reglamentos (UE) 2017/745 y (UE) 2017/746 establecen requisitos esenciales de ciberseguridad para los productos sanitarios que funcionan a través de un sistema electrónico o que son en sí mismos programas informáticos. Esos Reglamentos también abarcan algunos tipos de programas informáticos no incorporados y el enfoque global del ciclo de vida. Esos requisitos obligan a los fabricantes a desarrollar y crear sus productos aplicando principios de gestión de riesgos y estableciendo requisitos que tengan en cuenta las medidas de seguridad informática y los procedimientos de evaluación de la conformidad correspondientes. Además, desde diciembre de 2019 existen orientaciones específicas sobre la ciberseguridad de los productos sanitarios, que proporcionan a los fabricantes de productos sanitarios, incluidos los productos para diagnóstico in vitro, orientaciones relativas al cumplimiento de todos los requisitos esenciales de ciberseguridad pertinentes relativos a la ciberseguridad establecidos en el anexo I de dichos Reglamentos. Por lo tanto, a los productos con elementos digitales a los que se aplique alguno de esos Reglamentos no se les debe aplicar el presente Reglamento.

---

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

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

(26) Los productos con elementos digitales que se desarrollen o modifiquen exclusivamente con fines militares o de seguridad nacional o los productos que estén específicamente diseñados para procesar información clasificada no entrarán dentro del alcance del presente Reglamento. Se anima a los Estados miembros a que garanticen el mismo grado o uno mayor de protección para dichos productos que para aquellos entrantes en el alcance del presente Reglamento.

(27) El Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo[11] establece requisitos para la homologación de tipo de los vehículos, así como de sus sistemas y componentes, a cuyo fin introduce determinados requisitos de ciberseguridad, también relativos al funcionamiento de un sistema de gestión de la ciberseguridad certificado y a las actualizaciones de los programas informáticos; aborda las políticas y los procesos de las organizaciones en relación con los riesgos de ciberseguridad que afectan a todo el ciclo de vida de los vehículos, los equipos y los servicios, en consonancia con los reglamentos aplicables de las Naciones Unidas sobre especificaciones técnicas y ciberseguridad; en particular el Reglamento n.º 155 de las Naciones Unidas – Disposiciones uniformes relativas a la homologación de los vehículos de motor en lo que respecta a la ciberseguridad y al sistema de gestión de esta y establece procedimientos específicos de evaluación de la conformidad.

---

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

En el ámbito de la aviación, el principal objetivo del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo[12] es establecer y mantener un nivel elevado y uniforme de seguridad de la aviación civil en la Unión. Este Reglamento crea un marco para los requisitos esenciales de ciberseguridad de aeronavegabilidad de los productos, componentes y equipos aeronáuticos, incluidos los programas informáticos, que comprenden las obligaciones relativas a la protección contra las amenazas para la seguridad de la información. El proceso de certificación establecido en el Reglamento (UE) 2018/1139 garantiza el nivel de garantía al que aspira el presente Reglamento. Por consiguiente, los productos con elementos digitales a los que se aplica el Reglamento (UE) 2019/2144 y los productos certificados de conformidad con el Reglamento (UE) 2018/1139 no deben estar obligados a cumplir los requisitos esenciales de ciberseguridad ni se les deben aplicar los procedimientos de evaluación de la conformidad establecidos en el presente Reglamento.

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

(28) El presente Reglamento establece normas horizontales en materia de ciberseguridad que no son específicas de determinados sectores o productos con elementos digitales. No obstante, podrían introducirse normas de la Unión específicas por productos o sectores que establezcan requisitos que aborden la totalidad o parte de los riesgos cubiertos por los requisitos esenciales de ciberseguridad previstos en el presente Reglamento. En tales casos, la aplicación del presente Reglamento a los productos con elementos digitales a los que se apliquen otras normas de la Unión que establezcan requisitos que abordan la totalidad o parte de los riesgos cubiertos por los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento puede limitarse o excluirse siempre que dicha limitación o exclusión sea coherente con el marco regulador general aplicable a dichos productos y que las normas sectoriales alcancen como mínimo un nivel de protección equivalente al previsto en el presente Reglamento. La Comisión debe estar facultada para adoptar actos delegados para completar el presente Reglamento mediante la especificación de dichos productos y normas. El presente Reglamento incluye disposiciones específicas que aclaran su relación con el Derecho vigente de la Unión que implique la aplicación de tales limitaciones o exclusiones.

(29) Con el fin de garantizar que los productos con elementos digitales comercializados puedan repararse eficazmente y que su durabilidad se amplíe, debe disponerse una exención para los repuestos. Dicha exención deber referirse tanto a los repuestos concebidos para reparar productos heredados comercializados antes de la fecha de aplicación del presente Reglamento como para los repuestos que ya se hayan sometido a un procedimiento de evaluación de la conformidad con arreglo al presente Reglamento y que suministra el mismo fabricante.

(30) El Reglamento Delegado (UE) 2022/30 de la Comisión[13] especifica que ciertos requisitos esenciales de ciberseguridad establecidos en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE del Parlamento Europeo y del Consejo[14], relativa a los daños a la red y al uso inadecuado de los recursos de la red, la protección de los datos personales y la privacidad, y al fraude, se aplican a determinados equipos radioeléctricos. La Decisión de Ejecución C(2022) 5637 de la Comisión, de 5 de agosto de 2022, relativa a una solicitud de normalización presentada al Comité Europeo de Normalización y al Comité Europeo de Normalización Electrotécnica establece requisitos para la elaboración de normas específicas que detallan con mayor precisión cómo deben abordarse esos requisitos esenciales de ciberseguridad. Los requisitos esenciales de ciberseguridad previstos en el presente Reglamento incluyen todos los elementos de los requisitos esenciales de ciberseguridad contemplados en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE. Asimismo, los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento se ajustan a los objetivos de los requisitos de las normas específicas incluidos en dicha petición de normalización. Por tanto, cuando la Comisión deroga o modifica el Reglamento Delegado (UE) 2022/30 y, en consecuencia, este deja de aplicarse a determinados productos sujetos al presente Reglamento, la Comisión y las organizaciones europeas de normalización deben tener en cuenta el trabajo de normalización llevado a cabo en el contexto de la Decisión de Ejecución C(2022) 5637 en lo que respecta a la preparación y el desarrollo de normas armonizadas para facilitar la ejecución del presente Reglamento. Durante el período transitorio para la aplicación del presente Reglamento, la Comisión debe proporcionar orientaciones a los fabricantes a los que se aplica el presente Reglamento que también deban cumplir el Reglamento Delegado (UE) 2022/30 para facilitar la demostración del cumplimiento de ambos Reglamentos.

---

13 Reglamento Delegado (UE) 2022/30 de la Comisión, de 29 de octubre de 2021, que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, apartado 3, letras d), e) y f), de dicha Directiva (DO L 7 de 12.1.2022, p. 6).

14 Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62).

(31) La Directiva (UE) 2024/… del Parlamento Europeo y del Consejo[15+] se complementa con el presente Reglamento. Dicha Directiva establece normas en materia de responsabilidad por los daños causados por productos defectuosos, de forma que los perjudicados puedan reclamar una indemnización cuando hayan sufrido un daño derivado de dichos productos. Establece el principio de que el fabricante de un producto es responsable de los daños causados por la falta de seguridad de su producto, con independencia de la eventual existencia de culpa («responsabilidad objetiva»). Cuando dicha falta de seguridad consista en una falta de actualizaciones de seguridad posterior a la introducción del producto en el mercado, y esta cause daños, podría aplicarse la responsabilidad del fabricante. Las obligaciones de los fabricantes relativas a la provisión de actualizaciones de seguridad deben establecerse en el presente Reglamento.

---

15 Directiva (UE) …/… del Parlamento Europeo y del Consejo, de …, relativa a … (DO L, …, ELI: …).

\+ DO: insértese en el texto el número de la Directiva que figura en el documento PE-CONS 7/24[2022/0302(COD)] e insértese el número, la fecha, el título y la referencia al DO de dicha Directiva en la nota al pie de página.

(32) El presente Reglamento debe entenderse sin perjuicio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[16], incluidas las disposiciones relativas a la implantación de mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos a fin de demostrar la conformidad con ese Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. Este tipo de operaciones podrían integrarse en un producto con elementos digitales. La protección de datos desde el diseño y por defecto, así como la ciberseguridad en general, son elementos clave del Reglamento (UE) 2016/679. Al proteger a los consumidores y a las organizaciones de los riesgos de ciberseguridad, los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento también contribuyen a mejorar la protección de los datos personales y la privacidad de las personas. Deben tenerse en cuenta las sinergias tanto en materia de normalización como de certificación de los aspectos relativos a la ciberseguridad a través de la cooperación entre la Comisión, las organizaciones europeas de normalización, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Comité Europeo de Protección de Datos creado por el Reglamento (UE) 2016/679 y las autoridades nacionales de supervisión de la protección de datos. También deben fomentarse las sinergias entre el presente Reglamento y el Derecho de la Unión en materia de protección de datos en el ámbito de la vigilancia del mercado y la ejecución de las normas. A tal fin, las autoridades nacionales de vigilancia del mercado designadas con arreglo al presente Reglamento deben cooperar con las autoridades responsables de supervisar la aplicación del Derecho de la Unión en materia de protección de datos. Estas últimas también deben tener acceso a la información pertinente para el desempeño de sus tareas.

---

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

(33) En la medida en que sus productos entren en el ámbito de aplicación del presente Reglamento, los proveedores de carteras de identidad digital europea a que se refiere el artículo 5 *bis*, apartado 2, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo[17] deben cumplir tanto los requisitos esenciales de ciberseguridad horizontales establecidos en el presente Reglamento como los requisitos específicos de seguridad establecidos en el artículo 5 *bis* del Reglamento (UE) n.º 910/2014. A fin de facilitar el cumplimiento de sus obligaciones, los proveedores de carteras deben poder demostrar la conformidad de las carteras de identidad digital europea con los requisitos establecidos en el presente Reglamento y en el Reglamento (UE) n.º 910/2014, mediante la certificación de sus productos con arreglo a un esquema europeo de certificación de la ciberseguridad establecido con arreglo al Reglamento (UE) 2019/881 para el cual la Comisión haya especificado, mediante actos delegados una presunción de conformidad con el presente Reglamento, en la medida en que el certificado, o partes de este, abarque dichos requisitos.

---

[17] Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

(34) Al integrar componentes procedentes de terceros en productos con elementos digitales durante la fase de diseño y desarrollo, los fabricantes, a fin de garantizar que los productos se diseñen, desarrollen y produzcan de conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, deben ejercer la diligencia debida con respecto a dichos componentes, incluidos los componentes de programas informáticos libres y de código abierto que no se hayan comercializado. El nivel apropiado de diligencia debida depende de la naturaleza y del nivel de riesgo de ciberseguridad asociado a un componente concreto, y debe, a tal efecto, tener en cuenta una o varias de las acciones que siguen: verificar, según proceda, que el fabricante de un componente ha demostrado la conformidad con el presente Reglamento, también comprobando si el componente ya lleva el marcado CE; verificar que un componente recibe actualizaciones de seguridad periódicas, por ejemplo comprobando su historial de actualizaciones de seguridad; verificar que un componente está libre de vulnerabilidades registradas en la base de datos europea de vulnerabilidades establecida en virtud del artículo 12, apartado 2, de la Directiva (UE) 2022/2555 o en otras bases de datos de vulnerabilidades de acceso público; o realizar pruebas de seguridad adicionales. Las obligaciones de gestión de las vulnerabilidades establecidas en el presente Reglamento, que los fabricantes deben cumplir al introducir un producto con elementos digitales en el mercado y durante el período de soporte, se aplican a los productos con elementos digitales en su totalidad, incluidos todos los componentes integrados. Cuando, en el ejercicio de la diligencia debida, el fabricante del producto con elementos digitales identifique una vulnerabilidad en un componente, incluido un componente libre y de código abierto, debe informar a la persona o entidad que fabrique o mantenga el componente, abordar y corregir la vulnerabilidad y, en su caso, facilitar a la persona o entidad la solución de seguridad aplicada.

(35) Inmediatamente después del período transitorio para la aplicación del presente Reglamento, es posible que un fabricante de un producto con elementos digitales que integre uno o varios componentes procedentes de terceros a los que también se aplique el presente Reglamento no pueda verificar, como parte de su obligación de diligencia debida, que los fabricantes de dichos componentes han demostrado la conformidad con el presente Reglamento comprobando, por ejemplo, si los componentes ya llevan el marcado CE. Este puede ser el caso cuando los componentes se hayan integrado antes de que el presente Reglamento sea aplicable a los fabricantes de dichos componentes. En tal caso, un fabricante que integre dichos componentes debe ejercer la diligencia debida por otros medios.

(36) Los productos con elementos digitales deben llevar el marcado CE para acreditar de manera visible, legible e indeleble su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado de productos con elementos digitales que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE. Asimismo, los Estados miembros no impedirán que en ferias, exposiciones, demostraciones o actos similares se presenten o usen productos con elementos digitales que no sean conformes con el presente Reglamento, incluidos sus prototipos, a condición de que el producto se presente con una señal visible que indique claramente que el producto no es conforme con el presente Reglamento y no debe comercializarse hasta que lo sea.

(37) A fin de garantizar que los fabricantes puedan lanzar programas informáticos con fines de prueba antes de someter sus productos con elementos digitales a la evaluación de la conformidad, los Estados miembros no deben impedir la disponibilidad de programas informáticos incompletos, como versiones alfa, beta o candidatas a la publicación, siempre y cuando el programa informático inacabado solo se ponga a disposición durante el tiempo necesario para probarla y recabar información al respecto. Los fabricantes deben garantizar que los programas informáticos disponibles en esas condiciones solo sean lanzados una vez que se sometan a la evaluación de riesgos y que cumplan, en la medida de lo posible, los requisitos de seguridad relativos a las propiedades de los productos con elementos digitales previstos en el presente Reglamento. Los fabricantes también deben aplicar, en la medida de lo posible, los requisitos de gestión de las vulnerabilidades. Los fabricantes no deben obligar a los usuarios a actualizar las versiones publicadas únicamente a efectos de prueba.

(38) A fin de garantizar que los productos con elementos digitales no planteen riesgos de ciberseguridad para las personas y las organizaciones al ser introducidos en el mercado, deben establecerse requisitos esenciales de ciberseguridad para dichos productos. Estos requisitos esenciales de ciberseguridad, incluidos los requisitos de gestión de la vulnerabilidad, se aplican a cada producto individual con elementos digitales cuando se introduce en el mercado, independientemente de si el producto con elementos digitales se fabrica como una unidad individual o en serie. Por ejemplo, para un tipo de producto, cada producto con elementos digitales debe haber recibido todos los parches o actualizaciones de seguridad disponibles para abordar problemas de seguridad pertinentes cuando se introduzca en el mercado. Cuando los productos con elementos digitales se modifiquen posteriormente, por medios físicos o digitales, de una manera no prevista por el fabricante en la evaluación de riesgo inicial y que pueda implicar que dejen de cumplir los requisitos esenciales de ciberseguridad pertinentes, dicha modificación debe considerarse sustancial. Por ejemplo, las reparaciones pueden ser incluidas entre las operaciones de mantenimiento siempre que no modifiquen un producto con elementos digitales ya introducido en el mercado de tal manera que puedan afectar a su observancia de los requisitos vigentes o cambiar la finalidad prevista para el cual se ha evaluado el producto.

(39) Al igual que en el caso de las reparaciones o modificaciones físicas, un producto con elementos digitales debe considerarse sustancialmente modificado por un cambio en los programas informáticos cuando la actualización de los programas informáticos modifique la finalidad prevista para ese producto y esos cambios no estuviesen previstos por el fabricante en la evaluación del riesgo inicial; o cuando la naturaleza del peligro haya cambiado o el nivel de riesgo de ciberseguridad haya aumentado debido a la actualización del programa informático, y la versión actualizada del producto se comercialice. Cuando una actualización de seguridad, diseñada para reducir el nivel de riesgo de ciberseguridad de un producto con elementos digitales, no modifique la finalidad prevista de un producto con elementos digitales, no se considera una modificación sustancial. Ello suele incluir situaciones en las que las actualizaciones de seguridad solo implican ajustes menores del código fuente. Por ejemplo, este podría ser el caso cuando una actualización de seguridad aborde una vulnerabilidad conocida, también en el caso de que lo haga modificando funciones o el rendimiento de un producto con elementos digitales con el único fin de reducir el nivel de riesgo de ciberseguridad. Del mismo modo, una actualización de funcionalidad menor, como una mejora visual o la incorporación de nuevos pictogramas o nuevas lenguas a la interfaz de usuario, en general, no deben considerarse una modificación sustancial. Por el contrario, cuando una actualización de características modifique las funciones previstas originales o el tipo o el rendimiento de un producto con elementos digitales y cumpla dichos criterios, debe considerarse una modificación sustancial, ya que la incorporación de nuevas características suele dar lugar a una superficie de ataque más amplia, aumentando así el riesgo de ciberseguridad. Por ejemplo, este podría ser el caso cuando se añada un nuevo elemento de entrada a una solicitud que exija al fabricante que garantice una validación adecuada de los datos de entrada. A la hora de evaluar si una actualización de características se considera una modificación sustancial, no es pertinente si se presenta como actualización separada o en combinación con una actualización de seguridad. La Comisión debe emitir orientaciones sobre el modo de determinar lo que constituye una modificación sustancial.

(40) Teniendo en cuenta el carácter iterativo del desarrollo de programas informáticos, los fabricantes que hayan introducido en el mercado versiones posteriores de productos consistentes en programas informáticos como consecuencia de una posterior modificación sustancial de dicho producto deben poder proporcionar actualizaciones de seguridad durante el período de soporte únicamente para la versión del producto consistente en un programa informático que hayan introducido en el mercado por última vez. Solo deben poder hacerlo si los usuarios de las versiones anteriores pertinentes del producto tienen acceso gratuito a la versión del producto introducida por última vez en el mercado y no incurren en costes adicionales para adaptar el entorno de equipos o programas informáticos en el que operan el producto. Este podría ser el caso, por ejemplo, cuando la mejora del sistema operativo de mesa no requiera un nuevo equipo informático, como una unidad central de procesamiento más rápida o más memoria. No obstante, el fabricante debe seguir cumpliendo, durante el período de soporte, otros requisitos de gestión de vulnerabilidades, como disponer de una política de divulgación coordinada de vulnerabilidades o de medidas para facilitar el intercambio de información sobre posibles vulnerabilidades para todas las versiones posteriores sustancialmente modificadas del programa informático introducido en el mercado. Los fabricantes deben poder proporcionar actualizaciones menores de seguridad o funcionalidad que no constituyan una modificación sustancial únicamente de la última versión o subversión de un producto consistente en un programa informático que no haya sido modificado sustancialmente. Al mismo tiempo, cuando un producto consistente en un equipo informático, como un teléfono inteligente, no sea compatible con la última versión del sistema operativo con el que se entregó originalmente, el fabricante debe seguir proporcionando actualizaciones de seguridad al menos para la última versión compatible del sistema operativo durante el período de soporte.

(41) En consonancia con el concepto comúnmente establecido de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, cuando se produzca una modificación sustancial que pueda afectar al cumplimiento del presente Reglamento por parte del producto con elementos digitales o cuando la finalidad prevista del producto cambie, conviene que se verifique la conformidad del producto con elementos digitales y que, cuando proceda, se someta a una nueva evaluación de la conformidad. En su caso, si el fabricante lleva a cabo una evaluación de la conformidad en la que participa un tercero, deben notificarse a este último los cambios que puedan dar lugar a una modificación sustancial.

(42) Cuando un producto con elementos digitales sea objeto de «reacondicionamiento», «mantenimiento» y «reparación», tal como se define en el artículo 2, puntos 18, 19 y 20, del Reglamento (UE) 2024/1781 del Parlamento Europeo y el Consejo[18], ello no conduce necesariamente a una modificación sustancial del producto, por ejemplo, si la finalidad prevista y las funcionalidades no se modifican y el nivel de riesgo no se ve afectado. No obstante, la mejora de un producto con elementos digitales por parte del fabricante podría dar lugar a cambios en el diseño y el desarrollo del producto y podría, por tanto, afectar a su finalidad prevista y a la conformidad con los requisitos establecidos en el presente Reglamento.

---

18 Reglamento (UE) 2024/1781 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se instaura un marco para el establecimiento de requisitos de diseño ecológico aplicables a los productos sostenibles, se modifican la Directiva (UE) 2020/1828 y el Reglamento (UE) 2023/1542 y se deroga la Directiva 2009/125/CE (DO L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) El producto con elementos digitales debe considerarse importante si el impacto negativo de la explotación de las posibles vulnerabilidades del producto pueden ser graves, debido, por ejemplo, a la función vinculada a la ciberseguridad o a una función que entraña un riesgo significativo de efectos adversos en cuanto a su intensidad y su capacidad para perturbar, controlar o dañar un gran número de otros productos con elementos digitales, o la salud, la protección o la seguridad de sus usuarios, a través de una manipulación directa (por ejemplo, una función central del sistema, incluidos la gestión de la red, el control de la configuración, la virtualización o el tratamiento de datos personales). En particular, las vulnerabilidades de los productos con elementos digitales cuya funcionalidad está relacionada con la ciberseguridad, como los gestores de arranque, pueden llevar a una propagación de las cuestiones de seguridad a lo largo de la cadena de suministro. La gravedad del impacto de un incidente también puede aumentar cuando el producto desempeñe una función del sistema central, incluida la gestión de la red, el control de la configuración, la virtualización o el tratamiento de datos personales.

(44) Algunas categorías de productos con elementos digitales deben someterse a procedimientos de evaluación de la conformidad más estrictos, al tiempo que se garantiza un enfoque proporcionado. A tal fin, los productos importantes con elementos digitales deben dividirse en dos clases que reflejen el nivel de riesgo de ciberseguridad presente en esas categorías de productos. Un posible incidente de ciberseguridad que afecte a productos importantes con elementos digitales incluidos en la clase II podría dar lugar a mayores repercusiones negativas que un incidente que afecte a productos importantes con elementos digitales incluidos en la clase I, por ejemplo debido a la naturaleza de su función relacionada con la ciberseguridad o al desempeño de otra función que entrañe un riesgo significativo de efectos adversos. Como indicación de esa mayor repercusión negativa, los productos con elementos digitales incluidos en la clase II podrían desempeñar una funcionalidad relacionada con la ciberseguridad u otra función que entrañe un riesgo significativo de efectos adversos superior a los enumerados en la clase I, o bien cumplir ambos criterios. Por lo tanto, los productos importantes con elementos digitales incluidos en la clase II deben someterse a un procedimiento de evaluación de la conformidad más estricto.

(45) Los productos importantes con elementos digitales a que se refiere el presente Reglamento deben entenderse como productos que tienen la funcionalidad básica de una categoría de productos importantes con elementos digitales establecida en el presente Reglamento. Por ejemplo, el presente Reglamento establece categorías de productos importantes con elementos digitales que se definen por su funcionalidad principal como cortafuegos o sistemas de detección o prevención de intrusiones de la clase II. Como consecuencia de ello, los cortafuegos y sistemas de detección o prevención están sujetos a una evaluación de la conformidad por parte de terceros obligatoria. Esto no sucede con otros productos con elementos digitales no clasificados como productos importantes con elementos digitales que pueden llevar incorporados cortafuegos o sistemas de detección o prevención de intrusiones. La Comisión debe adoptar un acto de ejecución para especificar la descripción técnica de las categorías de productos importantes con elementos digitales incluidos en las clases I y II, tal como se dispone en el presente Reglamento.

(46) Las categorías de productos críticos con elementos digitales establecidas en el presente Reglamento tienen una funcionalidad relacionada con la ciberseguridad y desempeñan una función que conlleva un riesgo significativo de efectos adversos en términos de intensidad y capacidad para perturbar, controlar o dañar un gran número de otros productos con elementos digitales mediante manipulación directa. Además, estas categorías de productos con elementos digitales se consideran dependencias críticas de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555. Las categorías de productos críticos con elementos digitales establecidas en un anexo del presente Reglamento, debido a su carácter crítico, ya utilizan ampliamente diversas formas de certificación, y también están cubiertas por el esquema europeo de certificación de la ciberseguridad basado en criterios comunes establecidos en el Reglamento de Ejecución (UE) 2024/482 de la Comisión[19]. Por consiguiente, a fin de garantizar una protección común adecuada de la ciberseguridad de los productos críticos con elementos digitales en la Unión, podría ser adecuado y proporcionado someter dichas categorías de productos, mediante un acto delegado, a una certificación europea obligatoria de la ciberseguridad cuando ya exista un esquema europeo de certificación de la ciberseguridad pertinente que cubra esos productos y la Comisión haya llevado a cabo una evaluación del posible impacto en el mercado de la certificación obligatoria prevista. Dicha evaluación debe tener en cuenta tanto el lado de la oferta como el de la demanda, también si existe una demanda suficiente de los productos con elementos digitales de que se trate tanto de los Estados miembros como de los usuarios para exigir el certificado europeo de ciberseguridad, así como las finalidades previstas para los que se pretende utilizar los productos con elementos digitales, como las dependencias críticas de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555. La evaluación también debe analizar los posibles efectos de la certificación obligatoria en la disponibilidad de dichos productos en el mercado interior y las capacidades y la preparación de los Estados miembros para la aplicación de los esquemas europeos de certificación de la ciberseguridad pertinentes.

---

[19] Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Los actos delegados que exijan un certificado europeo obligatoria de la ciberseguridad deben determinar los productos con elementos digitales que tienen la funcionalidad básica de una categoría de productos críticos con elementos digitales establecida en el presente Reglamento que deben estar sujetos a certificación obligatoria, así como el nivel de garantía requerido, que debe ser como mínimo «sustancial». El nivel de garantía requerido debe ser proporcional al nivel de riesgo de ciberseguridad asociado al producto con elementos digitales. Por ejemplo, si el producto con elementos digitales tiene la funcionalidad básica de una categoría de productos críticos con elementos digitales establecida en el presente Reglamento y está destinado al uso en un entorno sensible o crítico, como los productos destinados al uso de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555, puede requerir el nivel de garantía más alto.

(48) A fin de garantizar una protección común adecuada de la ciberseguridad en la Unión de los productos con elementos digitales que tengan la funcionalidad básica de una categoría de productos críticos con elementos digitales establecida en el presente Reglamento, la Comisión también debe estar facultada para adoptar actos delegados que modifiquen el presente Reglamento añadiendo o retirando categorías de productos críticos con elementos digitales para los que los fabricantes podrían estar obligados a obtener un certificado europeo de ciberseguridad en virtud de un esquema europeo de certificación de la ciberseguridad en virtud del Reglamento (UE) 2019/881 para demostrar la conformidad con el presente Reglamento. Puede añadirse a dichas categorías una nueva categoría de productos críticos con elementos digitales si existe una dependencia crítica de ellos por parte de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555 o, si se ven afectadas por incidentes o al contener vulnerabilidades aprovechadas, esto podría dar lugar a perturbaciones de las cadenas de suministro críticas. Al evaluar la necesidad de añadir o retirar categorías de productos críticos con elementos digitales mediante un acto delegado, la Comisión debe poder tener en cuenta si los Estados miembros han identificado a nivel nacional productos con elementos digitales que desempeñan un papel fundamental para la resiliencia de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555 y que se enfrentan cada vez más a ciberataques en la cadena de suministro, con posibles efectos perturbadores graves. Asimismo, la Comisión debe poder tener en cuenta los resultados de las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión llevadas a cabo de conformidad con el artículo 22 de la Directiva (UE) 2022/2555.

(49) La Comisión debe asegurarse de que se consulte de manera estructurada y periódica a una amplia gama de partes interesadas pertinentes a la hora de preparar las medidas para la aplicación del presente Reglamento. Este debe ser el caso, en particular, cuando la Comisión evalúe la necesidad de posibles actualizaciones de las listas de categorías de productos importantes o críticos con elementos digitales, cuando se consulte a los fabricantes pertinentes y se tengan en cuenta sus puntos de vista para analizar los riesgos de ciberseguridad, así como el equilibrio de costes y beneficios de designar tales categorías de productos como importantes o críticos.

(50) El presente Reglamento aborda los riesgos de ciberseguridad de una manera específica. Sin embargo, los productos con elementos digitales podrían plantear otros riesgos para la seguridad en ocasiones ajenos a la ciberseguridad pero que pueden obedecer a una infracción de la seguridad. Estos riesgos deben seguir estando regulados por la legislación de armonización de la Unión pertinente distinta del presente Reglamento. Si no es aplicable ninguna legislación de armonización de la Unión distinta del presente Reglamento, debe estar sujeta al Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo[20]. Por consiguiente, habida cuenta del carácter específico del presente Reglamento, no obstante lo dispuesto en el artículo 2, apartado 1, párrafo tercero, letra b), del Reglamento (UE) 2023/988, el capítulo III, sección 1, los capítulos V y VII y los capítulos IX a XI del Reglamento (UE) 2023/988 deben ser aplicables a los productos con elementos digitales en lo que respecta a los riesgos para la seguridad no contemplados en el presente Reglamento, a condición de que dichos productos no estén sujetos a requisitos específicos impuestos por otra legislación de armonización de la Unión, aparte de este Reglamento, a los efectos del artículo 3, punto 27, del Reglamento (UE) 2023/988.

---

[20] Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (DO L 135 de 23.5.2023, p. 1).

(51) Los productos con elementos digitales considerados sistemas de inteligencia artificial (IA) de alto riesgo en virtud del artículo 6 del Reglamento (UE) 2024/1689 del Parlamento Europeo y el Consejo[21] que entren en el ámbito de aplicación del presente Reglamento deben cumplir los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. Cuando estos sistemas de IA de alto riesgo cumplan los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, debe considerarse que cumplen los requisitos de ciberseguridad establecidos en el artículo 15 del Reglamento (UE) 2024/1689 en la medida en que dichos requisitos estén contemplados en la declaración UE de conformidad expedida en virtud del presente Reglamento o en partes de esta. A tal efecto, la evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales clasificado como un sistema de IA de alto riesgo de conformidad con el Reglamento (UE) 2024/1689 que debe tenerse en cuenta durante las fases de planificación, diseño, desarrollo, producción, entrega y mantenimiento del producto con elementos digitales, con arreglo a lo previsto por el presente Reglamento, deben tener en cuenta los riesgos de ciberresiliencia de un sistema de IA en lo relativo a los intentos de terceros no autorizados de alterar su uso, comportamiento o desempeño, incluidas las vulnerabilidades específicas de la IA como el envenenamiento de datos o los ataques adversarios, así como los riesgos pertinentes para los derechos fundamentales, de conformidad con el Reglamento (UE) 2024/1689. Por lo que se refiere a los procedimientos de evaluación de la conformidad relativos a los requisitos esenciales de ciberseguridad de un producto con elementos digitales que entra dentro del ámbito de aplicación del presente Reglamento y considerado sistema de IA de alto riesgo, las disposiciones pertinentes del artículo 43 del Reglamento (UE) 2024/1689 deben aplicarse como norma general en lugar de las disposiciones pertinentes del presente Reglamento.

---

[21] 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).

Sin embargo, esta regla no debe dar lugar a una reducción del nivel de garantía necesario para los productos importantes o críticos con elementos digitales tal como se menciona en el presente Reglamento. Por consiguiente, como excepción a lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento (UE) 2024/1689, que asimismo se consideren productos importantes o críticos con elementos digitales tal como se menciona en el presente Reglamento y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno especificado en el anexo VI del Reglamento (UE) 2024/1689 deben estar sujetos a las procedimientos relativos a la evaluación de la conformidad incluidos en el presente Reglamento en la medida en que se refieran a los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. En este caso, para todos los demás aspectos que entren en el ámbito de aplicación del Reglamento (UE) 2024/1689, deben aplicarse las disposiciones pertinentes sobre la evaluación de la conformidad basadas en el control interno establecidas en el anexo VI de dicho Reglamento.

(52) Para mejorar la seguridad de los productos con elementos digitales comercializados en el mercado interior, es necesario establecer requisitos esenciales de ciberseguridad aplicables a esos productos. Esos requisitos esenciales de ciberseguridad deben entenderse sin perjuicio de las evaluaciones coordinadas de los riesgos de seguridad a escala de la Unión que se efectúen con respecto a las cadenas de suministro críticas previstas en el artículo 22 de la Directiva (UE) 2022/2555, que tienen en cuenta factores de riesgo tanto técnicos como, cuando proceda, de otra índole, por ejemplo la influencia indebida de un tercer país sobre los proveedores. Además, sin perjuicio de las prerrogativas de los Estados miembros y con el fin de garantizar un alto nivel de resiliencia, deben establecerse requisitos adicionales que tengan en cuenta los factores no técnicos, incluidos los definidos en la Recomendación (UE) 2019/534 de la Comisión[22], en la evaluación coordinada de riesgos de la ciberseguridad a escala de la Unión de la seguridad de las redes 5G y en el conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G acordado por el Grupo de Cooperación establecido en virtud del artículo 14 la Directiva (UE) 2022/2555.

[22] Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G (DO L 88 de 29.3.2019, p. 42).

(53) Los fabricantes de productos incluidos en el ámbito de aplicación del Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo[23] que sean también productos con elementos digitales en el sentido del presente Reglamento deben cumplir tanto los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento como los requisitos esenciales de ciberseguridad de salud y seguridad establecidos en el Reglamento (UE) 2023/1230. Los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento y determinados requisitos esenciales de ciberseguridad establecidos en el Reglamento (UE) 2023/1230 podrían abordar riesgos de ciberseguridad similares. Por consiguiente, el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento podría facilitar el cumplimiento de los requisitos esenciales de ciberseguridad que también cubren determinados riesgos de ciberseguridad establecidos en el Reglamento (UE) 2023/1230, y en particular los relativos a la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de control establecidos en el anexo III, secciones 1.1.9 y 1.2.1, de ese Reglamento. El fabricante debe demostrar tales sinergias, por ejemplo, aplicando, cuando estén disponibles, normas armonizadas u otras especificaciones técnicas que abarquen los requisitos esenciales de ciberseguridad pertinentes tras una evaluación de riesgos que incluya esos riesgos de ciberseguridad. El fabricante también debe seguir los procedimientos de evaluación de la conformidad aplicables establecidos en el presente Reglamento y en el Reglamento (UE) 2023/1230. La Comisión y las organizaciones europeas de normalización, en los trabajos preparatorios que apoyan la aplicación del presente Reglamento y del Reglamento (UE) 2023/1230 y los procesos de normalización conexos, deben promover la coherencia en la forma en que deben evaluarse los riesgos de ciberseguridad y en la forma en que esos riesgos deben ser cubiertos por las normas armonizadas con respecto a los requisitos esenciales de ciberseguridad pertinentes.

---

[23] Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo (DO L 165 de 29.6.2023, p. 1).

En particular, la Comisión y las organizaciones europeas de normalización deben tener en cuenta el presente Reglamento en la preparación y el desarrollo de normas armonizadas para facilitar la aplicación del Reglamento (UE) 2023/1230 en lo que respecta, en particular, a los aspectos de ciberseguridad relacionados con la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de control establecidos en el anexo III, secciones 1.1.9 y 1.2.1, de ese Reglamento. La Comisión debe proporcionar orientaciones para ayudar a los fabricantes a los que se aplique el presente Reglamento que también deban cumplir lo dispuesto en el Reglamento (UE) 2023/1230, en particular para facilitar la demostración de la conformidad con los requisitos esenciales de ciberseguridad pertinentes establecidos en el presente Reglamento y en el Reglamento (UE) 2023/1230.

(54) Para garantizar que los productos con elementos digitales sean seguros tanto en el momento de su introducción en el mercado como durante el tiempo que esté previsto utilizar el producto con elementos digitales, es necesario establecer requisitos esenciales de ciberseguridad para la gestión de las vulnerabilidades y requisitos esenciales de ciberseguridad de ciberseguridad relativos a las propiedades de los productos con elementos digitales. Si bien los fabricantes deben cumplir todos los requisitos esenciales de ciberseguridad en relación con la gestión de las vulnerabilidades a través del período de soporte a lo largo de todo el período de soporte, también deben determinar qué otros requisitos esenciales de ciberseguridad relacionados con las propiedades del producto son pertinentes para el tipo de producto con elementos digitales de que se trate. A tal fin, los fabricantes deben llevar a cabo una evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales para determinar los riesgos y los requisitos esenciales de ciberseguridad pertinentes, para ofrecer sus productos con elementos digitales sin vulnerabilidades aprovechables conocidas que puedan incidir en su seguridad y aplicar adecuadamente las normas armonizadas, especificaciones comunes o normas internacionales o europeas apropiadas.

(55) Cuando determinados requisitos esenciales de ciberseguridad no sean aplicables a un producto con elementos digitales, el fabricante debe incluir una justificación clara en la evaluación del riesgo de ciberseguridad incluido en la documentación técnica. Este podría ser el caso cuando un requisito esencial sea incompatible con la naturaleza de un producto con elementos digitales. Por ejemplo, la finalidad prevista de un producto con elementos digitales puede requerir que el fabricante siga normas de interoperabilidad ampliamente reconocidas, incluso si sus características de seguridad ya no se consideran de última tecnología. Del mismo modo, otra normativa de la Unión exige a los fabricantes que apliquen requisitos específicos de interoperabilidad. Cuando un requisito esencial no sea aplicable a un producto con elementos digitales, pero el fabricante haya identificado riesgos de ciberseguridad en relación con dicho requisito esencial, debe adoptar medidas para hacer frente a dichos riesgos por otros medios, por ejemplo, limitando la finalidad prevista del producto a entornos de confianza o informando a los usuarios de dichos riesgos.

(56) Una de las medidas más importantes que deben adoptar los usuarios para proteger sus productos con elementos digitales de los ciberataques es instalar las últimas actualizaciones de seguridad disponibles lo antes posible. Por consiguiente, los fabricantes deben diseñar sus productos y poner en marcha procesos para garantizar que los productos con elementos digitales incluyan funciones que permitan la notificación, distribución, descarga e instalación de actualizaciones de seguridad automáticamente, en particular en el caso de los productos de consumo. También deben ofrecer la posibilidad de aprobar la descarga y la instalación de las actualizaciones de seguridad como paso final. Los usuarios deben conservar la capacidad de desactivar las actualizaciones automáticas, con un mecanismo claro y fácil de utilizar, respaldado por instrucciones claras sobre cómo pueden renunciar los usuarios. Los requisitos relativos a las actualizaciones automáticas establecidos en un anexo del presente Reglamento no son aplicables a los productos con elementos digitales destinados principalmente a integrarse como componentes en otros productos. Tampoco se aplican a los productos con elementos digitales para los que los usuarios no esperarían razonablemente actualizaciones automáticas, incluidos los productos con elementos digitales destinados a ser utilizados en redes profesionales de TIC, y especialmente en entornos críticos e industriales en los que una actualización automática podría causar interferencias con las operaciones. Con independencia de si un producto con elementos digitales está diseñado para recibir actualizaciones automáticas o no, su fabricante debe informar a los usuarios sobre las vulnerabilidades y poner a disposición las actualizaciones de seguridad sin demora. Cuando un producto con elementos digitales tenga una interfaz de usuario o medios técnicos similares que permitan una interacción directa con sus usuarios, el fabricante debe hacer uso de dichas características para informar a los usuarios de que su producto con elementos digitales ha alcanzado el final del período de soporte. Las notificaciones deben limitarse a lo necesario para garantizar la recepción efectiva de esta información y no deben tener una repercusión negativa en la experiencia del usuario del producto con elementos digitales.

(57) Para mejorar la transparencia de los procesos de gestión de las vulnerabilidades y garantizar que los usuarios no estén obligados a instalar nuevas actualizaciones de funcionalidad con el único fin de recibir las últimas actualizaciones de seguridad, los fabricantes deben garantizar, cuando sea técnicamente viable, que las nuevas actualizaciones de seguridad se proporcionen por separado de las actualizaciones de funcionalidad.

(58) En la Comunicación conjunta de la Comisión y del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 20 de junio de 2023, titulada «Estrategia Europea de Seguridad Económica», se afirmaba que la Unión debe maximizar los beneficios de su apertura económica, minimizando al mismo tiempo los riesgos derivados de la dependencia económica de los proveedores de alto riesgo, a través de un marco estratégico común para la seguridad económica de la Unión. Las dependencias respecto a proveedores de alto riesgo de productos con elementos digitales entrañan un riesgo estratégico que debe abordarse a escala de la Unión, especialmente cuando los productos con elementos digitales se han concebido para su uso por entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555. Tales riesgos pueden estar vinculados al órgano jurisdiccional al que está sujeto el fabricante, a las características de su titularidad corporativa y los vínculos de control con el gobierno de un tercer país en el que se encuentre establecido, en particular si un país tercero lleva a cabo actividades de espionaje económico y su legislación permite el acceso arbitrario a todo tipo de operaciones o datos empresariales, incluidos los datos comercialmente sensibles, y puede imponer obligaciones con fines de inteligencia sin controles ni equilibrios democráticos, mecanismos de supervisión, garantías procesales o el derecho de recurso ante un órgano jurisdiccional independiente. Al determinar la importancia de un riesgo de ciberseguridad de acuerdo con lo previsto en el presente Reglamento, la Comisión y las autoridades de vigilancia del mercado también tendrán en cuenta los factores de riesgo no técnicos, en particular los establecidos como resultado de las evaluaciones coordinadas de riesgos para la seguridad de las cadenas de suministro críticas a escala de la Unión realizadas de conformidad con el artículo 22 de la Directiva (UE) 2022/2555.

(59) Con el fin de garantizar la seguridad de los productos con elementos digitales tras su introducción en el mercado, los fabricantes deben determinar un período de soporte, que deben reflejar el tiempo que se espera que el producto con elementos digitales esté en uso. Al determinar un período de soporte, el fabricante debe tener en cuenta, en particular, las expectativas razonables de los usuarios, la naturaleza del producto, así como la legislación pertinente de la Unión que determina la vida útil de los productos con elementos digitales. Los fabricantes también deben poder tener en cuenta otros factores pertinentes. Los criterios deben aplicarse de manera que se garantice la proporcionalidad en la determinación de los períodos de soporte. Previa solicitud, un fabricante debe facilitar a las autoridades de vigilancia del mercado la información que se ha tenido en cuenta para determinar el período de soporte de un producto con elementos digitales.

(60) El período de soporte durante el cual el fabricante garantiza la gestión eficaz de las vulnerabilidades no debe ser inferior a cinco años, a menos que la vida útil del producto con elementos digitales sea inferior a cinco años, en cuyo caso el fabricante debe garantizar la gestión de la vulnerabilidad durante dicha vida útil. Cuando el tiempo de utilización del producto con elementos digitales sea superior a cinco años, como suele ocurrir en el caso de los componentes de equipo informático, como placas madre o microprocesadores, dispositivos de red como enrutadores, módems o conmutadores, así como programas informáticos, como sistemas operativos o herramientas de edición de vídeo, los fabricantes deben garantizar en consecuencia períodos de soporte más largos. En particular, los productos con elementos digitales destinados a ser utilizados en entornos industriales, como los sistemas de control industrial, suelen utilizarse durante períodos de tiempo mucho más largos. Un fabricante solo debe poder definir un período de soporte inferior a cinco años cuando así lo justifique la naturaleza del producto con elementos digitales de que se trate y cuando se prevea que dicho producto se utilice durante menos de cinco años, en cuyo caso el período de soporte debe corresponder al tiempo de uso previsto. Por ejemplo, la vida útil de una aplicación de rastreo de contactos destinada a utilizarse durante una pandemia podría limitarse a la duración de la pandemia. Además, algunas aplicaciones informáticas solo pueden ponerse a disposición, por naturaleza, sobre la base de un modelo de suscripción, en particular cuando la aplicación deja de estar disponible para el usuario y, por consiguiente, ya no se utiliza una vez que caduque la suscripción.

(61) Cuando los productos con elementos digitales alcancen el final de sus períodos de soporte, a fin de garantizar que las vulnerabilidades puedan tratarse una vez finalizado el período de soporte, los fabricantes deben considerar la posibilidad de divulgar el código fuente de dichos productos con elementos digitales a otras empresas que se comprometan a ampliar la prestación de servicios de gestión de vulnerabilidades o al público. Cuando los fabricantes divulguen el código fuente a otras empresas, deben poder proteger la propiedad del producto con elementos digitales e impedir la difusión del código fuente al público, por ejemplo mediante acuerdos contractuales.

(62) A fin de garantizar que los fabricantes de toda la Unión determinen períodos de soporte similares para productos comparables con elementos digitales, el ADCO debe publicar estadísticas sobre los períodos de soporte medios determinados por los fabricantes para las categorías de productos con elementos digitales y publicar orientaciones que indiquen períodos de soporte adecuados para dichas categorías. Además, con vistas a garantizar un enfoque armonizado en todo el mercado interior, la Comisión debe poder adoptar actos delegados para especificar períodos mínimos de soporte para categorías específicas de productos cuando los datos facilitados por las autoridades de vigilancia del mercado sugieran que los períodos de soporte determinados por los fabricantes o bien no se ajustan sistemáticamente a los criterios para determinar los períodos de soporte establecidos en el presente Reglamento, o bien que los fabricantes de diferentes Estados miembros determinan injustificadamente diferentes períodos de soporte.

(63) Los fabricantes deben establecer un punto de contacto único que permita a los usuarios comunicarse fácilmente con ellos, también con el fin de notificar y recibir información sobre las vulnerabilidades del producto con elemento digital. Deben hacer que el punto de contacto único sea fácilmente accesible para los usuarios e indicar claramente su disponibilidad, manteniendo esta información actualizada. Cuando los fabricantes opten por ofrecer herramientas automatizadas, por ejemplo, cajas de chat, también deben ofrecer un número de teléfono u otros medios digitales de contacto, como una dirección de correo electrónico o un formulario de contacto. El punto de contacto único no debe basarse exclusivamente en herramientas automatizadas.

(64) Los fabricantes deben comercializar sus productos con elementos digitales con una configuración segura por defecto y proporcionar actualizaciones de seguridad a los usuarios de forma gratuita. Los fabricantes solo deben poder apartarse de esos requisitos esenciales de ciberseguridad en relación con los productos adaptados que se ajusten a un fin particular para una determinada empresa y cuando tanto el fabricante como el usuario hayan acordado explícitamente un conjunto diferente de condiciones contractuales.

(65) Los fabricantes deben notificar simultáneamente, a través de la plataforma única de notificación, tanto al equipo de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) designado como coordinador, así como a la ENISA, las vulnerabilidades aprovechadas activamente contenidas en productos con elementos digitales, así como los incidentes graves que repercutan en la seguridad de esos productos. Las notificaciones deben presentarse utilizando el punto final de notificación electrónica de un CSIRT designado como coordinador y deben ser accesibles simultáneamente para la ENISA.

(66) Los fabricantes deben notificar las vulnerabilidades aprovechadas activamente para garantizar que los CSIRT designados como coordinadores y la ENISA tengan una visión de conjunto adecuada de esas vulnerabilidades y reciban la información necesaria para desempeñar sus tareas, tal como se establece en la Directiva (UE) 2022/2555, aumentar el nivel general de ciberseguridad de las entidades esenciales e importantes a que se refiere el artículo 3 de dicha Directiva, así como para garantizar el funcionamiento eficaz de las autoridades de vigilancia del mercado. Dado que la mayoría de los productos con elementos digitales se comercializan en todo el mercado interior, cualquier vulnerabilidad aprovechada en un producto con elementos digitales debe considerarse una amenaza para el funcionamiento del mercado interior. La ENISA, de acuerdo con el fabricante, debe divulgar vulnerabilidades solucionadas a la base de datos europea de vulnerabilidades creada de conformidad con el artículo 12, apartado 2, de la Directiva (UE) 2022/2555. La base de datos europea de vulnerabilidades ayudará a los fabricantes a detectar las vulnerabilidades aprovechables conocidas halladas en sus productos con el fin de asegurarse de que la comercialización de productos seguros.

(67) Los fabricantes también deben notificar cualquier incidente grave que repercuta en la seguridad del producto con elementos digitales al CSIRT designado como coordinador y a la ENISA. Para garantizar que los usuarios puedan reaccionar rápidamente ante incidentes graves que repercutan en la seguridad de sus productos con elementos digitales, los fabricantes también deben informar a sus usuarios sobre cualquier incidente de este tipo y, en su caso, sobre las medidas correctoras que los usuarios puedan adoptar para atenuar las repercusiones del incidente, por ejemplo, mediante la publicación de la información pertinente en sus sitios web o, cuando el fabricante pueda ponerse en contacto con los usuarios y los riesgos de ciberseguridad lo justifiquen, comunicándose directamente con ellos.

(68) Las vulnerabilidades aprovechadas activamente se refieren a casos en los que un fabricante establece que una violación de la seguridad que afecta a sus usuarios o a cualquier otra persona física o jurídica se debe a un agente malintencionado que hace uso de un defecto en uno de los productos con elementos digitales comercializados por el fabricante. Ejemplos de estas vulnerabilidades podrían ser deficiencias en las funciones de identificación y autenticación de un producto. Las vulnerabilidades que se descubren sin una intención maliciosa con fines de comprobación de buena fe, investigación, corrección o divulgación para promover la seguridad o la protección del propietario del sistema y sus usuarios no deben ser objeto de notificaciones obligatorias. Los incidentes graves que repercuten en la seguridad del producto con elementos digitales, por otra parte, se refieren a situaciones en las que un incidente de ciberseguridad afecta a los procesos de desarrollo, producción o mantenimiento del fabricante de manera que pueda dar lugar a un aumento del riesgo de ciberseguridad para los usuarios u otras personas. Es incidente grave puede consistir en una situación en la que un atacante haya comprometido con éxito el canal de publicación a través del que el fabricante hace llegar las actualizaciones de seguridad a los usuarios.

(69) Para garantizar que las notificaciones puedan difundirse rápidamente a todos los CSIRT pertinentes designados como coordinadores y para que los fabricantes puedan presentar una notificación única en cada fase del proceso de notificación, la ENISA debe establecer una plataforma única de notificación con puntos finales nacionales de notificación electrónica. La ENISA debe gestionar y mantener las operaciones cotidianas de esa plataforma única de notificación. Los CSIRT designados como coordinadores deben informar a sus respectivas autoridades de vigilancia del mercado sobre las vulnerabilidades o incidentes notificados. La plataforma única de notificación debe diseñarse de manera que garantice la confidencialidad de las notificaciones, en particular en lo que respecta a las vulnerabilidades para las que todavía no se dispone de una actualización de seguridad. Además, la ENISA debe establecer procedimientos para tratar la información de manera segura y confidencial. Sobre la base de la información que recopile, la ENISA debe elaborar un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en productos con elementos digitales y presentarlo al Grupo de Cooperación establecido en virtud del artículo 14 de la Directiva (UE) 2022/2555.

(70) En circunstancias excepcionales, y en particular a petición del fabricante, el CSIRT designado como coordinador que reciba inicialmente una notificación debe poder decidir retrasar su difusión a los demás CSIRT pertinentes designados como coordinadores a través de la plataforma única de notificación cuando ello pueda justificarse por motivos relacionados con la ciberseguridad y durante un período de tiempo estrictamente necesario. El CSIRT designado como coordinador debe informar inmediatamente a la ENISA sobre la decisión de retrasar y por qué motivos, así como sobre cuándo tiene la intención de seguir difundiendo. La Comisión debe elaborar, mediante un acto delegado, especificaciones sobre las condiciones para cuándo podrían aplicarse los motivos relacionados con la ciberseguridad y debe cooperar con la red de CSIRT establecida en virtud del artículo 15 de la Directiva (UE) 2022/2555 y con la ENISA en la preparación del proyecto de acto delegado. Algunos ejemplos de motivos relacionados con la ciberseguridad son un procedimiento coordinado de divulgación de vulnerabilidades en curso o situaciones en las que se espera que un fabricante proporcione una medida correctora en breve y los riesgos de ciberseguridad de una difusión inmediata a través de la plataforma única de notificación compensan con creces sus beneficios. Si así lo solicita el CSIRT designado como coordinador, la ENISA debe poder apoyar a dicho CSIRT en la aplicación de motivos relacionados con la ciberseguridad en relación con el aplazamiento de la difusión de la notificación sobre la base de la información que la ENISA haya recibido de ese CSIRT sobre la decisión de denegar una notificación por esos motivos de ciberseguridad. Además, en circunstancias especialmente excepcionales, la ENISA no debe recibir todos los detalles de una notificación de vulnerabilidad aprovechada activamente de manera simultánea.

Este sería el caso cuando el fabricante señale en su notificación que la vulnerabilidad notificada ha sido aprovechada activamente por un agente malintencionado y que, según la información disponible, no ha sido aprovechada en otro Estado miembro distinto del CSIRT designado como coordinador al que el fabricante haya notificado la vulnerabilidad, cuando cualquier difusión ulterior inmediata de la vulnerabilidad notificada pueda dar lugar probablemente a que se facilite información cuya divulgación sea contraria a los intereses esenciales de dicho Estado miembro, o cuando la vulnerabilidad notificada plantee un riesgo de ciberseguridad elevado inminente derivado de la ulterior difusión. En tales casos, la ENISA solo recibirá acceso simultáneo a la información de que el fabricante ha realizado una notificación, información general sobre el producto con elementos digitales de que se trate, información sobre el carácter general del aprovechamiento de la vulnerabilidad e información sobre el hecho de que dichos motivos de seguridad fueron planteados por el fabricante y, por tanto, no se divulga todo el contenido de la notificación. La notificación completa debe entonces ponerse a disposición de la ENISA y de otros CSIRT pertinentes designados como coordinadores cuando el CSIRT designado inicialmente como coordinador que recibió la notificación considere que esos motivos de seguridad, que reflejan circunstancias especialmente excepcionales, tal como se establecen en el presente Reglamento, dejan de existir. Cuando, sobre la base de la información citada, la ENISA considere que existe un riesgo sistémico que afecta a la seguridad en el mercado interior, recomendará al CSIRT receptor que difunda la notificación completa a los demás CSIRT designados como coordinadores y a la propia ENISA.

(71) Cuando los fabricantes notifiquen una vulnerabilidad aprovechada activamente o un incidente grave que afecte a la seguridad de un producto con elementos digitales, deben indicar en qué medida consideran sensible la información notificada. El CSIRT designado como coordinador que recibe inicialmente la notificación debe tener en cuenta esta información a la hora de evaluar si la notificación da lugar a circunstancias excepcionales que justifiquen un retraso en la difusión de la notificación a los demás CSIRT pertinentes designados como coordinadores por motivos justificados relacionados con la ciberseguridad. También debe tener en cuenta esta información a la hora de evaluar si la notificación de una vulnerabilidad aprovechada activamente da lugar a circunstancias especialmente excepcionales que justifiquen que la notificación completa no se ponga simultáneamente a disposición de la ENISA. Por último, los CSIRT designados como coordinadores deben poder tener en cuenta dicha información a la hora de determinar las medidas adecuadas para atenuar los riesgos derivados de tales vulnerabilidades e incidentes.

(72) A fin de simplificar la notificación de la información requerida en virtud del presente Reglamento, teniendo en cuenta otros requisitos complementarios de presentación de informes establecidos en el Derecho de la Unión, como el Reglamento (UE) 2016/679, el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo[24], la Directiva 2002/58/CE del Parlamento Europeo y del Consejo[25] y la Directiva (UE) 2022/2555, así como para reducir la carga administrativa para las entidades, se anima a los Estados miembros a que consideren la posibilidad de establecer a nivel nacional puntos de entrada únicos para esos requisitos de información. El uso de dicho punto de entrada único para la notificación de incidentes de seguridad con arreglo al Reglamento (UE) 2016/679 y a la Directiva 2002/58/CE no debe afectar a la aplicación de las disposiciones del Reglamento (UE) 2016/679 y de la Directiva 2002/58/CE, en particular las relativas a la independencia de las autoridades a que estos actos se refieren. Al establecer la plataforma única de notificación a que se refiere el presente Reglamento, la ENISA debe tener en cuenta la posibilidad de que los puntos finales nacionales de notificación electrónica a que se refiere el presente Reglamento se integren en los puntos de entrada únicos nacionales, que también pueden integrar otras notificaciones exigidas por el Derecho de la Unión.

---

[24] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333 de 27.12.2022, p. 1).

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

(73) Al establecer la plataforma única de notificación a que se refiere el presente Reglamento y con el fin de aprovechar la experiencia adquirida, la ENISA debe consultar a otras instituciones o agencias de la Unión que gestionan plataformas o bases de datos sujetas a estrictos requisitos de seguridad, como la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA). La ENISA debe también analizar la posible complementariedad con la base de datos europea de vulnerabilidades establecida en virtud del artículo 12, apartado 2, de la Directiva (UE) 2022/2555.

(74) Los fabricantes y otras personas físicas y jurídicas deben poder notificar a un CSIRT designado como coordinador o a la ENISA, de forma voluntaria, cualquier vulnerabilidad contenida en un producto con elementos digitales, ciberamenazas que puedan afectar al perfil de riesgo de un producto con elementos digitales, cualquier incidente que afecte a la seguridad de un producto con elementos digitales, así como cuasiincidentes que puedan haber dado lugar a dicho incidente.

(75) Los Estados miembros deben tener como objetivo abordar, en la medida de lo posible, los retos a que se enfrentan los investigadores de vulnerabilidades, incluida la posibilidad de incurrir en responsabilidad penal, de conformidad con el Derecho nacional. Dado que las personas físicas y jurídicas que investigan vulnerabilidades podrían incurrir en algunos Estados miembros en responsabilidad civil y penal, se alienta a los Estados miembros a que adopten directrices para que no se actúe penalmente cuando se trate de investigadores de seguridad de la información y que no se exija responsabilidad civil por sus actividades.

(76) Los fabricantes de productos con elementos digitales deben establecer políticas de divulgación coordinada de las vulnerabilidades para facilitar la notificación de vulnerabilidades por parte de particulares o entidades, ya sea directamente al fabricante o indirectamente, y cuando se requiera de forma anónima, a través de CSIRT designados coordinadores a efectos de la divulgación coordinada de vulnerabilidades de conformidad con el artículo 12, apartado 1, de la Directiva (UE) 2022/2555. Una política de divulgación coordinada de vulnerabilidades de los fabricantes debe especificar un proceso estructurado a través del cual las vulnerabilidades se notifican al fabricante de tal manera que este pueda diagnosticar y subsanar las vulnerabilidades antes de que se revele información detallada sobre ellas a terceros o al público. Además, los fabricantes también deben considerar la posibilidad de publicar sus políticas de seguridad en un formato legible por máquina. Dado que la información sobre vulnerabilidades aprovechables en productos de uso generalizado con elementos digitales puede venderse a precios elevados en el mercado negro, los fabricantes de estos productos, como parte de sus políticas de divulgación coordinada de vulnerabilidades, deben poder utilizar programas para incentivar la notificación de vulnerabilidades, garantizando que las personas o las entidades reciban reconocimiento y compensación por sus esfuerzos. Esto atañe a los denominados «programas de recompensa por detección de errores» o «bug bounty».

(77) A fin de facilitar el análisis de las vulnerabilidades, los fabricantes deben especificar y documentar los componentes contenidos en los productos con elementos digitales, también mediante la elaboración de una SBOM. Una SBOM puede proporcionar a quienes fabrican, compran y utilizan dichos programas información que mejore su comprensión de la cadena de suministro, lo que tiene múltiples beneficios, en particular ayuda a los fabricantes y a los usuarios a rastrear las vulnerabilidades y los riesgos de ciberseguridad conocidos de reciente aparición. Es de particular importancia que los fabricantes garanticen que sus productos con elementos digitales no contengan componentes vulnerables desarrollados por terceros. Los fabricantes no deben estar obligados a hacer pública la SBOM.

(78) Conforme a los nuevos modelos de negocio complejos vinculados a las ventas en línea, una empresa que opere en línea puede prestar diversos servicios. Dependiendo de la naturaleza de los servicios prestados en relación con un determinado producto con elementos digitales, la misma entidad puede pertenecer a diferentes categorías de modelos de negocio u operadores económicos. Cuando una entidad presta servicios de intermediación en línea respecto a un producto concreto con elementos digitales y es sencillamente proveedora de un mercado en línea, conforme se define en el artículo 3, apartado 14, del Reglamento (UE) 2023/988, no puede ser considerada operador económico conforme se define en el presente Reglamento. Cuando una misma entidad sea proveedora de un mercado en línea y también ejerza como operador económico tal como se define en el presente Reglamento respecto a la venta de productos con elementos digitales, debe someterse a las obligaciones establecidas en el presente Reglamento para ese tipo de operador económico. Por ejemplo, si el proveedor del mercado en línea también distribuye un producto con elementos digitales, entonces, con respecto a la venta de ese producto, se le consideraría un distribuidor. Del mismo modo, si la entidad en cuestión vende sus propios productos con elementos digitales de marca actuaría como fabricante y, por tanto, tendría que cumplir los requisitos aplicables a los fabricantes. Asimismo, algunas entidades pueden considerarse prestadores de servicios logísticos, tal como se definen en el artículo 3, punto 11, del Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo[26], si ofrecen tales servicios. Estos casos tendrían que evaluarse caso por caso. Habida cuenta del papel destacado que desempeñan los mercados en línea en la posibilitación del comercio electrónico, deben esforzarse por cooperar con las autoridades de vigilancia del mercado de los Estados miembros con el fin de asegurarse de que los productos con elementos digitales adquiridos en esos mercados en línea se atengan a los requisitos de ciberseguridad formulados en el presente Reglamento.

---

[26] Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 (DO L 169 de 25.6.2019, p. 1).

(79) A fin de facilitar la evaluación de la conformidad con los requisitos establecidos en el presente Reglamento, debe aplicarse una presunción de conformidad de los productos con elementos digitales que sean conformes con normas armonizadas que plasmen los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento en especificaciones técnicas detalladas y se adopten de conformidad con el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[27]. Ese Reglamento establece un procedimiento de presentación de objeciones a las normas armonizadas para el caso en que estas no cumplan plenamente los requisitos establecidos en el presente Reglamento. El proceso de normalización debe garantizar una representación equilibrada de intereses y la participación efectiva de las partes interesadas de la sociedad civil, incluidas las organizaciones de consumidores. También deben tenerse en cuenta las normas internacionales que estén en consonancia con el nivel de protección de la ciberseguridad perseguido por los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, a fin de facilitar el desarrollo de normas armonizadas y la aplicación del presente Reglamento, así como de facilitar el cumplimiento por parte de las empresas, en particular las microempresas y las pequeñas y medianas empresas, y las que operan a escala mundial.

---

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

(80) El desarrollo oportuno de normas armonizadas durante el período transitorio para la aplicación del presente Reglamento y la disponibilidad antes de la fecha de aplicación del presente Reglamento serán especialmente importantes para su aplicación efectiva. Esto es, en particular, el caso de los productos con elementos digitales importantes que entran dentro de la clase I. La disponibilidad de las normas armonizadas permitirá a los fabricantes de esos productos llevar a cabo evaluaciones de la conformidad a través del procedimiento de control interno y, por consiguiente, puede evitar los cuellos de botella y los retrasos en las actividades de los organismos de evaluación de la conformidad.

(81) El Reglamento (UE) 2019/881 establece un marco europeo voluntario de certificación de la ciberseguridad para productos, procesos y servicios de TIC. Los esquemas europeos de certificación de la ciberseguridad pueden proporcionar un marco común de confianza para que los usuarios utilicen los productos con elementos digitales que entren dentro del ámbito de aplicación del presente Reglamento. El presente Reglamento debe crear por consiguiente sinergias con el Reglamento (UE) 2019/881. A fin de facilitar la evaluación de la conformidad con los requisitos establecidos en el presente Reglamento, se presupondrá que los productos con elementos digitales que hayan sido certificados o para los que se haya expedido una declaración de conformidad en el marco de un esquema europeo de ciberseguridad establecido en virtud del Reglamento (UE) 2019/881 y reconocido por la Comisión mediante acto de ejecución son conformes con los requisitos esenciales de ciberseguridad del presente Reglamento en la medida en que el certificado europeo de ciberseguridad o la declaración de conformidad, o partes de estos, cubran dichos requisitos. La necesidad de nuevos esquemas europeos de certificación de la ciberseguridad para productos con elementos digitales debe evaluarse a la luz del presente Reglamento, también al preparar programa de trabajo evolutivo de la Unión de conformidad con el Reglamento (UE) 2019/881. Cuando sea necesario un nuevo esquema que abarque los productos con elementos digitales, también para facilitar el cumplimiento del presente Reglamento, la Comisión podrá solicitar a la ENISA que prepare propuestas de esquema de conformidad con el artículo 48 del Reglamento (UE) 2019/881. Estos futuros esquemas europeos de certificación de la ciberseguridad que se apliquen a productos con elementos digitales deben tener en cuenta los requisitos esenciales de ciberseguridad y los procedimientos de evaluación de la conformidad establecidos en el presente Reglamento y facilitar su cumplimiento. En el caso de los esquemas europeos de certificación de la ciberseguridad que entren en vigor antes de la entrada en vigor del presente Reglamento, pueden ser necesarias especificaciones adicionales sobre aspectos detallados de cómo puede aplicarse una presunción de conformidad.

La Comisión, a través de actos delegados, debe estar facultada para especificar en qué condiciones los esquemas europeos de certificación de la ciberseguridad puedan utilizarse para demostrar la conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. Además, con el fin de evitar cargas administrativas excesivas para los fabricantes, no debería haber obligación alguna para los fabricantes de llevar a cabo una evaluación de la conformidad por parte de terceros, tal como dispone el presente Reglamento para los requisitos correspondientes cuando se haya expedido un certificado de ciberseguridad europeo en el marco de dichos esquemas europeos de certificación de la ciberseguridad, en un nivel sustancial o alto.

(82) Tras la entrada en vigor del Reglamento de Ejecución (UE) 2024/482 que se refiere a los productos que entran dentro del ámbito de aplicación del presente Reglamento, como los módulos de seguridad del hardware (HSM) y los microprocesadores de los equipos informáticos, la Comisión debe poder especificar, mediante un acto delegado, el modo en que el esquema europeo de certificación de la ciberseguridad supone la presunción de conformidad con los requisitos esenciales de ciberseguridad especificados en el presente Reglamento o partes de estos. Además, dicho acto delegado podrá especificar la medida en que un certificado expedido con arreglo al esquema europeo de certificación de la ciberseguridad exime a los fabricantes de la obligación de llevar a cabo una evaluación de terceros, tal como exige el presente Reglamento para los requisitos correspondientes.

(83) El actual marco de normalización europeo, que se basa en los principios del nuevo enfoque establecidos en la Resolución del Consejo de 7 de mayo de 1985 relativa a una nueva aproximación en materia de armonización y de normalización y en el Reglamento (UE) n.º 1025/2012, representa el marco por defecto para elaborar normas que prevean una presunción de conformidad con los requisitos esenciales de ciberseguridad pertinentes del presente Reglamento. Las normas europeas deben estar orientadas al mercado y tener en cuenta el interés público, así como los objetivos estratégicos claramente enunciados en la solicitud de la Comisión a una o varias organizaciones europeas de normalización para que elaboren normas armonizadas dentro de un plazo determinado y a partir del consenso. No obstante, en ausencia de referencias pertinentes a normas armonizadas, la Comisión debe poder adoptar actos de ejecución que establezcan especificaciones comunes relativas a los requisitos esenciales de ciberseguridad que establece el presente Reglamento, siempre que al hacerlo respete debidamente el papel y las funciones de los organismos de normalización, como solución alternativa excepcional para facilitar la obligación del fabricante de cumplir esos requisitos esenciales de ciberseguridad, o cuando el proceso de normalización esté bloqueado o cuando se produzcan retrasos en el establecimiento de normas armonizadas adecuadas. Si dichos retrasos se deben a la complejidad técnica de la norma en cuestión, la Comisión debe tenerlo en cuenta antes de considerar si procede establecer especificaciones comunes.

(84) Con vistas a establecer, de la manera más eficiente, especificaciones comunes que comprendan los requisitos esenciales de ciberseguridad de diseño ecológico que establece el presente Reglamento, la Comisión debe implicar proceso a las partes interesadas pertinentes.

(85) Por «período razonable» debe entenderse, en relación con la publicación de la referencia a normas armonizadas en el *Diario Oficial de la Unión Europea* de conformidad con el Reglamento (UE) n.º 1025/2012, un período durante el cual se espera la publicación en el *Diario Oficial de la Unión Europea* de la referencia a la norma, su corrección de errores o su modificación, y que no debe exceder de un año después de la fecha límite para la elaboración de una norma europea establecida de conformidad con el Reglamento (UE) n.º 1025/2012.

(86) Para facilitar la evaluación de la conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, debe presuponerse la conformidad de los productos con elementos digitales que sean conformes con las especificaciones comunes adoptadas por la Comisión con arreglo al presente Reglamento a fin de indicar las especificaciones técnicas detalladas de dichos requisitos.

(87) La aplicación de normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que aporten una presunción de conformidad en relación con los requisitos esenciales de ciberseguridad aplicables a los productos con elementos digitales facilitará la evaluación de la conformidad por parte de los fabricantes. Si el fabricante opta por no aplicar tales medios a determinados requisitos, ha de indicar en su documentación técnica cómo se alcanza la conformidad de otro modo. Además, la aplicación de normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que reconozcan una presunción de conformidad por parte de los fabricantes facilitaría el control de la conformidad de los productos con elementos digitales por parte de las autoridades de vigilancia del mercado. Por consiguiente, se anima a los fabricantes de productos con elementos digitales a aplicar dichas normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad.

(88) Los fabricantes deben elaborar una declaración UE de conformidad a fin de aportar la información requerida por el presente Reglamento sobre la conformidad de los productos con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento y, cuando proceda, en otra legislación de armonización de la Unión aplicable al producto con elementos digitales. También puede obligarse a los fabricantes a preparar una declaración UE de conformidad con arreglo a otros actos jurídicos de la Unión. Para garantizar un acceso efectivo a la información con fines de vigilancia del mercado, debe prepararse una única declaración UE de conformidad relativa al cumplimiento de todos los actos jurídicos pertinentes de la Unión. A fin de reducir las cargas administrativas para los operadores económicos, dicha declaración única de la UE ha de poder consistir en un expediente compuesto por cada una de las correspondientes declaraciones de conformidad.

(89) El marcado CE, que indica la conformidad de un producto, es el resultado visible de todo un proceso que comprende la evaluación de la conformidad en sentido amplio. Los principios generales por los que se rige el marcado CE se establecen en el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo[28]. En el presente Reglamento deben establecerse normas relativas a la colocación del marcado CE en productos con elementos digitales. El marcado CE debe ser el único marcado que garantice que los productos con elementos digitales cumplen con los requisitos establecidos en el presente Reglamento.

---

[28] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

(90) Para que los operadores económicos puedan demostrar la conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento y para que las autoridades de vigilancia del mercado puedan garantizar que los productos con elementos digitales comercializados cumplen dichos requisitos, es necesario establecer procedimientos de evaluación de la conformidad. La Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo[29] establece módulos de procedimientos de evaluación de la conformidad proporcionales al nivel de riesgo existente y al nivel de seguridad requerido. Para garantizar la coherencia intersectorial y evitar variantes *ad hoc*, los procedimientos de evaluación de la conformidad adecuados para verificar la conformidad de los productos con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento se deben basar en dichos módulos. Los procedimientos de evaluación de la conformidad deben examinar y verificar los requisitos relacionados con los productos y los procesos que abarcan todo el ciclo de vida de los productos con elementos digitales, incluidos la planificación, el diseño, el desarrollo o la producción, las pruebas y el mantenimiento del producto con elementos digitales.

[29] Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

(91) La evaluación de la conformidad de los productos con elementos digitales que no figuren en la lista de productos importantes o críticos con elementos digitales en el presente Reglamento podrá ser realizada por el fabricante bajo su propia responsabilidad siguiendo el procedimiento de control interno basado en el módulo A de la Decisión n.º 768/2008/CE, de conformidad con el presente Reglamento. Esto también se aplica a los casos en que un fabricante opte por no aplicar total o parcialmente una norma armonizada, una especificación común o un esquema europeo de certificación de la ciberseguridad aplicable. El fabricante mantiene la opción de elegir un procedimiento de evaluación de la conformidad más estricto en el que participe un tercero. En el marco del procedimiento de evaluación de la conformidad de control interno, el fabricante garantiza y declara, bajo su exclusiva responsabilidad, que el producto con elementos digitales y los procesos del fabricante cumplen los requisitos esenciales de ciberseguridad aplicables establecidos en el presente Reglamento. Si un producto importante con elementos digitales entra dentro de la clase I, se requieren garantías adicionales para demostrar la conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. Si el fabricante desea llevar a cabo la evaluación de la conformidad bajo su propia responsabilidad (módulo A), debe aplicar normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que hayan sido reconocidos por la Comisión mediante un acto de ejecución. Si el fabricante no aplica estas normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad, debe someterse a una evaluación de la conformidad en la que participe un tercero (basado en los módulos B y C o H). Teniendo en cuenta la carga administrativa de los fabricantes y el hecho de que la ciberseguridad desempeña un papel importante en la fase de diseño y desarrollo de productos tangibles e intangibles con elementos digitales, los procedimientos de evaluación de la conformidad basados, respectivamente, en los módulos B y C o H de la Decisión n.º 768/2008/CE han sido elegidos como los más adecuados para evaluar la conformidad de los productos con elementos digitales importantes de manera proporcionada y eficaz.

El fabricante que opte por la evaluación de la conformidad de terceros puede elegir el procedimiento que se adapte mejor a su proceso de diseño y producción. Dado el riesgo de ciberseguridad aún mayor vinculado al uso de productos con elementos digitales importantes incluidos en la clase II, la evaluación de la conformidad debe implicar siempre a un tercero, incluso cuando el producto cumpla total o parcialmente las normas armonizadas, las especificaciones comunes o los esquemas europeos de certificación de la ciberseguridad. Los fabricantes de productos importantes con elementos digitales que se consideren programas informáticos libres y de código abierto deben poder seguir el procedimiento de control interno basado en el módulo A, siempre que pongan la documentación técnica a disposición del público.

(92) Si bien la creación de productos tangibles con elementos digitales suele exigir a los fabricantes un esfuerzo considerable a lo largo de las fases de diseño, desarrollo y producción, la creación de productos con elementos digitales en forma de programas informáticos se centra casi exclusivamente en el diseño y el desarrollo, mientras que la fase de producción desempeña un papel menor. No obstante, en muchos casos, los productos consistentes en programas informáticos aún tienen que compilarse, integrarse, empaquetarse, hacerse disponibles para su descarga o copiarse en soportes físicos antes de su introducción en el mercado. Estas actividades deben considerarse como equivalentes a la fase de producción cuando se apliquen los módulos de evaluación de la conformidad pertinentes para verificar la conformidad del producto con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento a lo largo de las fases de diseño, desarrollo y producción.

(93) En relación con las microempresas y las pequeñas empresas, a fin de garantizar la proporcionalidad, conviene aligerar los costes administrativos sin afectar al nivel de protección de la ciberseguridad de los productos con elementos digitales que entran en el ámbito de aplicación del presente Reglamento o a la igualdad de condiciones entre fabricantes. Procede, por tanto, que la Comisión establezca un formulario simplificado de documentación técnica dirigido a las necesidades de las microempresas y las pequeñas empresas. El formulario simplificado de documentación técnica adoptado por la Comisión debe abarcar todos los elementos aplicables relacionados con la documentación técnica establecidos en el presente Reglamento y especificar cómo una microempresa o una pequeña empresa puede proporcionar los elementos solicitados de manera concisa, como la descripción del diseño, el desarrollo y la producción del producto con elementos digitales. De este modo, el formulario contribuiría a aliviar la carga administrativa de cumplimiento proporcionando a las empresas afectadas seguridad jurídica sobre el alcance y el detalle de la información que debe facilitarse. Las microempresas y las pequeñas empresas deben poder optar por proporcionar los elementos aplicables relacionados con la documentación técnica de forma amplia y no aprovechar la forma técnica simplificada de que disponen.

(94) Con el fin de promover y proteger la innovación, es importante que se tengan especialmente en cuenta los intereses de los fabricantes que sean microempresas o pequeñas o medianas empresas, en particular microempresas y pequeñas empresas, incluidas las empresas emergentes. A tal fin, los Estados miembros podrían desarrollar iniciativas dirigidas a fabricantes que sean microempresas o pequeñas empresas, también en materia de formación, sensibilización, comunicación de información, pruebas y actividades de evaluación de la conformidad por terceros, así como la creación de espacios controlados de pruebas. Los costes de traducción relacionados con la documentación obligatoria, como la documentación técnica y la información y las instrucciones para el usuario exigidas en virtud del presente Reglamento, y la comunicación con las autoridades, pueden constituir un coste significativo para los fabricantes, en particular los de menor tamaño. Por consiguiente, los Estados miembros deben tener la posibilidad de considerar que una de las lenguas en las que determinen y acepten que los fabricantes presenten la documentación pertinente y que pueda usarse para la comunicación con los fabricantes sea una lengua ampliamente conocida por el mayor número posible de usuarios.

(95) Con el fin de garantizar una aplicación fluida del presente Reglamento, los Estados miembros deben esforzarse por garantizar, antes de la fecha de aplicación del presente Reglamento, que existe un número suficiente de organismos notificados en la Unión para llevar a cabo las evaluaciones de la conformidad de terceros. La Comisión debe asistir a los Estados miembros y otras partes pertinentes en esta labor, con el fin de evitar los cuellos de botella y los obstáculos de los fabricantes a la entrada al mercado. Las actividades de formación específicas dirigidas por los Estados miembros, también, cuando proceda, con el apoyo de la Comisión, pueden contribuir a la disponibilidad de profesionales cualificados, incluido el apoyo a las actividades de los organismos notificados en virtud del presente Reglamento. Además, teniendo en cuenta los costes que puede entrañar la evaluación de la conformidad por parte de terceros, deben considerarse iniciativas de financiación a escala nacional y de la Unión destinadas a aliviar dichos costes para las microempresas y las pequeñas empresas.

(96) A fin de garantizar la proporcionalidad, los organismos de evaluación de la conformidad, al fijar las tarifas por los procedimientos de evaluación de la conformidad, deben tener en cuenta los intereses y necesidades específicos de las microempresas y las pequeñas y medianas empresas, incluidas las empresas emergentes. En particular, los organismos de evaluación de la conformidad solo deben aplicar el procedimiento de examen y las pruebas pertinentes previstos en el presente Reglamento cuando proceda y siguiendo un enfoque basado en el riesgo.

(97) Los objetivos de los espacios controlados de pruebas deben ser fomentar la innovación y la competitividad de las empresas mediante el establecimiento de entornos de prueba controlados antes de la introducción en el mercado de productos con elementos digitales. Los espacios controlados de pruebas deben contribuir a mejorar la seguridad jurídica para todos los operadores que entran en el ámbito de aplicación del presente Reglamento y facilitar y acelerar el acceso al mercado de la Unión de los productos con elementos digitales, en particular cuando los suministren microempresas y pequeñas empresas, incluidas las empresas emergentes.

(98) Las autoridades notificantes nacionales deben informar a la Comisión y a los demás Estados miembros acerca de los organismos que realizarán la evaluación de la conformidad por parte de terceros de los productos con elementos digitales, siempre y cuando cumplan una serie de requisitos, en particular en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses.

(99) Para garantizar un mismo nivel de calidad en la evaluación de la conformidad de los productos con elementos digitales, también es necesario establecer los requisitos que deben cumplir las autoridades notificantes y otros organismos que participen en la evaluación, la notificación y la supervisión de los organismos notificados. El sistema que dispone el presente Reglamento debe complementarse con el sistema de acreditación establecido en el Reglamento (CE) n.º 765/2008. Puesto que la acreditación es un medio esencial para comprobar la competencia de los organismos de evaluación de la conformidad, debe utilizarse también a efectos de notificación.

(100) Los organismos de evaluación de la conformidad que hayan sido acreditados y notificados con arreglo al Derecho de la Unión que establezcan requisitos similares a los establecidos en el presente Reglamento, como un organismo de evaluación de la conformidad que haya sido notificado para un esquema europeo de certificación de la ciberseguridad adoptado en virtud del Reglamento (UE) 2019/881 o notificado con arreglo al Reglamento Delegado (UE) 2022/30, deben ser evaluados de nuevo y notificados con arreglo al presente Reglamento. Sin embargo, las autoridades competentes pueden definir sinergias en relación con cualquier requisito que se solape, a fin de evitar una carga financiera y administrativa innecesaria, así como garantizar un proceso de notificación fluido y oportuno.

(101) Una acreditación transparente como la prevista en el Reglamento (CE) n.º 765/2008, que garantice el nivel de confianza necesario en los certificados de conformidad, debe ser considerada por las autoridades públicas nacionales de toda la Unión la forma más adecuada de demostrar la competencia técnica de dichos organismos de evaluación. No obstante, las autoridades nacionales pueden considerar que poseen los medios adecuados para llevar a cabo esa evaluación por sí mismas. En tal caso, con el fin de garantizar que las evaluaciones realizadas por otras autoridades nacionales tengan un grado adecuado de credibilidad, estas autoridades deben proporcionar a la Comisión y a los demás Estados miembros las pruebas documentales necesarias de que los organismos de evaluación de la conformidad evaluados cumplen los requisitos normativos aplicables.

(102) Es frecuente que los organismos de evaluación de la conformidad subcontraten parte de sus actividades relacionadas con la evaluación de la conformidad o que recurran a una filial. A fin de salvaguardar el nivel de protección exigido para la introducción en el mercado de productos con elementos digitales, es esencial que los subcontratistas y las filiales que evalúen la conformidad cumplan los mismos requisitos que los organismos notificados en cuanto a la realización de las tareas de evaluación de la conformidad.

(103) La autoridad notificante debe enviar la notificación de un organismo de evaluación de la conformidad a la Comisión y a los demás Estados miembros a través del Sistema de información sobre organismos notificados y designados de nuevo enfoque (NANDO, por sus siglas en inglés). El Sistema de información NANDO es la herramienta de notificación electrónica desarrollada y gestionada por la Comisión, y en ella se puede encontrar una lista de todos los organismos notificados.

(104) Dado que los organismos notificados pueden ofrecer sus servicios en toda la Unión, procede ofrecer a los demás Estados miembros y a la Comisión la oportunidad de presentar objeciones a propósito de un organismo notificado. Por lo tanto, es importante fijar un plazo durante el que se pueda aclarar cualquier duda o preocupación sobre la competencia de los organismos de evaluación de la conformidad antes de que empiecen a trabajar como organismos notificados.

(105) En aras de la competitividad, es fundamental que los organismos notificados apliquen los procedimientos de evaluación de la conformidad sin crear cargas innecesarias para los operadores económicos. Por el mismo motivo y para garantizar la igualdad de trato a esos operadores, debe garantizarse que la aplicación técnica de los procedimientos de evaluación de la conformidad sea uniforme. La mejor manera de lograrlo es instaurar una coordinación y una cooperación adecuadas entre los organismos notificados.

(106) La vigilancia del mercado es un instrumento esencial para garantizar la aplicación correcta y uniforme del Derecho de la Unión. Por lo tanto, es oportuno establecer un marco jurídico en el que pueda llevarse a cabo la vigilancia del mercado de manera apropiada. Las normas sobre vigilancia del mercado de la Unión y control de los productos que entran en el mercado de la Unión establecidas en el Reglamento (UE) 2019/1020 se aplican a los productos con elementos digitales que entran dentro del ámbito de aplicación del presente Reglamento.

(107) De conformidad con el Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado efectúan la vigilancia del mercado en el territorio del Estado miembro que las designe. El presente Reglamento no debe impedir que los Estados miembros elijan a las autoridades competentes para desempeñar funciones de vigilancia del mercado. Cada Estado miembro debe designar a una o varias autoridades de vigilancia del mercado en su territorio. Los Estados miembros deben poder optar por designar a cualquier autoridad existente o nueva para que actúe en calidad de autoridad de vigilancia del mercado, incluidas las autoridades nacionales competentes designadas o especificadas en virtud del artículo 8 de la Directiva (UE) 2022/2555 y las autoridades nacionales de certificación de la ciberseguridad designadas en virtud del artículo 58 del Reglamento (UE) 2019/881 o las autoridades de vigilancia del mercado designadas a efectos de la Directiva 2014/53/UE. Los operadores económicos deben cooperar plenamente con las autoridades de vigilancia del mercado y otras autoridades competentes. Cada Estado miembro debe informar a la Comisión y a los demás Estados miembros acerca de sus autoridades de vigilancia del mercado y de los ámbitos de competencia de cada una de ellas, así como garantizar las capacidades y los recursos necesarios para desempeñar las funciones de vigilancia del mercado relacionadas con el presente Reglamento. En virtud del artículo 10, apartados 2 y 3, del Reglamento (UE) 2019/1020, cada Estado miembro debe designar una oficina de enlace única que debe ser responsable de, entre otras cosas, representar la posición coordinada de las autoridades de vigilancia del mercado y prestar asistencia en la cooperación entre las autoridades de vigilancia del mercado en diferentes Estados miembros.

(108) Debe establecerse un Grupo de Cooperación Administrativa (ADCO, por sus siglas en inglés) específico en relación con la ciberresiliencia de los productos con elementos digitales para la aplicación uniforme del presente Reglamento, de conformidad con el artículo 30, apartado 2, del Reglamento (UE) 2019/1020. El ADCO debe estar compuesto por representantes de las autoridades de vigilancia del mercado designadas y, en su caso, por representantes de las oficinas de enlace únicas. La Comisión debe apoyar y fomentar la cooperación entre las autoridades de vigilancia del mercado a través de la Red de la Unión sobre Conformidad de los Productos, establecida en virtud del artículo 29 del Reglamento (UE) 2019/1020 y compuesta por representantes de cada Estado miembro, incluidos un representante de cada oficina de enlace única a que se refiere el artículo 10 del citado Reglamento y un experto nacional opcional, los presidentes de los ADCO y representantes de la Comisión. La Comisión debe participar en las reuniones de la Red de la Unión sobre Conformidad de los Productos, sus subgrupos y el ADCO. También debe ayudar al ADCO por medio de una secretaría ejecutiva que preste apoyo técnico y logístico. El ADCO también podrá invitar a participar a expertos independientes y servir de enlace con otros ADCO, como el establecido con arreglo a la Directiva 2014/53/UE.

(109) Las autoridades de vigilancia del mercado, a través del ADCO establecido con arreglo al presente Reglamento, deben cooperar estrechamente y deben poder elaborar documentos de orientación para facilitar las actividades de vigilancia del mercado a nivel nacional, por ejemplo, mediante el desarrollo de mejores prácticas e indicadores para comprobar eficazmente la conformidad de los productos con elementos digitales con el presente Reglamento.

(110) A fin de garantizar el establecimiento de medidas oportunas, proporcionadas y eficaces en relación con los productos con elementos digitales que presenten un riesgo de ciberseguridad significativo, debe preverse un procedimiento de salvaguardia de la Unión con arreglo al cual se informe a las partes interesadas de las medidas que se vayan a adoptar en relación con dichos productos. También debe permitir a las autoridades de vigilancia del mercado actuar, en cooperación con los operadores económicos correspondientes, en una fase más temprana cuando sea necesario. Si los Estados miembros y la Comisión están de acuerdo en la justificación de una medida adoptada por un Estado miembro, no debe exigirse mayor intervención de la Comisión excepto en los casos en los que la no conformidad pueda atribuirse a la insuficiencia de una norma armonizada.

(111) En determinados casos, un producto con elementos digitales que cumpla lo dispuesto en el presente Reglamento puede, no obstante, presentar un riesgo de ciberseguridad significativo o plantear un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones en virtud del Derecho nacional o de la Unión en materia de protección de los derechos fundamentales, para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema electrónico de información por entidades esenciales contempladas en el artículo 3, apartado 1, de la Directiva (UE) 2022/2555 o para otros aspectos relativos a la protección del interés público. Es por tanto necesario establecer normas que garanticen la reducción de estos riesgos. En consecuencia, las autoridades de vigilancia del mercado deben adoptar medidas para exigir al operador económico que se asegure de que el producto ya no presenta dicho riesgo, que lo retire del mercado o que lo recupere, dependiendo del riesgo que presente. Tan pronto como una autoridad de vigilancia del mercado restrinja o prohíba la libre circulación de un producto con elementos digitales de esa manera, el Estado miembro debe notificar inmediatamente a la Comisión y a los demás Estados miembros las medidas provisionales, indicando las razones y la justificación de esa decisión. Cuando una autoridad de vigilancia del mercado adopte tales medidas contra productos con elementos digitales que planteen un riesgo, la Comisión debe consultar sin demora a los Estados miembros y al operador o los operadores económicos pertinentes y debe evaluar la medida nacional. Basándose en los resultados de dicha evaluación, la Comisión debe decidir si la medida nacional está o no justificada. La Comisión debe comunicar inmediatamente su decisión a todos los Estados miembros y al operador o los operadores económicos pertinentes. Si la medida se considera justificada, la Comisión también debe considerar si adopta o no propuestas para revisar el Derecho de la Unión pertinente.

(112) Por lo que respecta a los productos con elementos digitales que presenten un riesgo de ciberseguridad significativo y en relación con los cuales existan motivos para creer que incumplen el presente Reglamento, o bien a los productos que cumplen el presente Reglamento pero presentan otros riesgos importantes, como riesgos para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones con arreglo al Derecho de la Unión o nacional en materia de protección de los derechos fundamentales o para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema de electrónico información por entidades esenciales contempladas en el artículo 3, apartado 1, de la Directiva (UE) 2022/2555, la Comisión debe poder solicitar a la ENISA que lleve a cabo una evaluación. Sobre la base de dicha evaluación, la Comisión debe poder adoptar, mediante actos de ejecución, medidas correctoras o restrictivas a escala de la Unión, como obligar a que los productos con elementos digitales de que se trate se retiren del mercado o se recuperen en un plazo razonable, proporcional a la naturaleza del riesgo. La Comisión solo debe poder recurrir a tal medida en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el correcto funcionamiento del mercado interior y únicamente cuando las autoridades de vigilancia del mercado no hayan adoptado medidas eficaces para subsanar la situación. Tales circunstancias excepcionales pueden darse en situaciones de emergencia en las que, por ejemplo, un fabricante comercialice de manera generalizada en varios Estados miembros un producto con elementos digitales no conforme utilizado asimismo en sectores clave por entidades que entren en el ámbito de aplicación de la Directiva (UE) 2022/2555, a pesar de contener vulnerabilidades conocidas que estén siendo aprovechadas por agentes malintencionados y para las que el fabricante no proporcione parches disponibles. La Comisión solo debe poder intervenir en situaciones de emergencia de este tipo mientras duren las circunstancias excepcionales y si persiste el incumplimiento del presente Reglamento o los riesgos importantes detectados.

(113) Cuando existan indicios de incumplimiento del presente Reglamento en varios Estados miembros, las autoridades de vigilancia del mercado deben poder llevar a cabo actividades conjuntas con otras autoridades, con el objetivo de verificar el cumplimiento y determinar los riesgos de ciberseguridad de los productos con elementos digitales.

(114) Las acciones de control simultáneas coordinadas («barridos») son medidas de ejecución específicas que las autoridades de vigilancia del mercado llevan a cabo para seguir mejorando la seguridad de los productos. En particular, deben llevarse a cabo barridos cuando las tendencias del mercado, las reclamaciones de los consumidores u otras indicaciones muestren que determinadas categorías de productos con elementos digitales presentan a menudo riesgos de ciberseguridad graves. Además, al determinar las categorías de productos para las que deben llegarse a cabo barridos, las autoridades de vigilancia del mercado también deben tener en cuenta circunstancias relacionadas con factores de riesgo no técnicos. A tal fin, las autoridades de vigilancia del mercado deben poder tener en cuenta los resultados de las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión llevadas a cabo de conformidad con el artículo 22 de la Directiva (UE) 2022/2555, incluidas circunstancias relativas a factores de riesgo no técnicos. La ENISA debe presentar a las autoridades de vigilancia del mercado propuestas de categorías de productos con elementos digitales para las que podrían organizarse barridos, sobre la base, entre otras cosas, de las notificaciones de vulnerabilidades e incidentes que reciba.

(115) En vista de sus conocimientos técnicos y su mandato, la ENISA debe poder apoyar el proceso de ejecución del presente Reglamento. En particular, la ENISA debe ser capaz de proponer actividades conjuntas que las autoridades de vigilancia del mercado deban llevar a cabo sobre la base de indicaciones o información sobre el posible incumplimiento del presente Reglamento por parte de productos con elementos digitales en varios Estados miembros, o de determinar categorías de productos para las que deban organizarse barridos. En circunstancias excepcionales que requieran una intervención inmediata para preservar el correcto funcionamiento del mercado interior, la ENISA, a petición de la Comisión, debe poder llevar a cabo evaluaciones relativas a productos específicos con elementos digitales que presenten un riesgo de ciberseguridad significativo.

(116) El presente Reglamento encomienda a la ENISA determinadas tareas que requieren recursos adecuados tanto en términos de conocimientos especializados como de recursos humanos para que la ENISA pueda llevarlas a cabo de manera eficaz. Al preparar el proyecto de presupuesto general de la Unión, la Comisión propondrá los recursos presupuestarios necesarios para la plantilla de personal de la ENISA, de conformidad con el procedimiento establecido en el artículo 29 del Reglamento (UE) 2019/881. En ese proceso, la Comisión tomará en consideración los recursos globales de la ENISA que le permitan desempeñar sus tareas, incluidas las que se le encomiendan en virtud del presente Reglamento.

(117) A fin de garantizar que el marco regulador pueda adaptarse cuando sea necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo a lo dispuesto en el artículo 290 del Tratado de Funcionamiento de la Unión Europea (TFUE) a efectos de actualizar e incluir en la lista del anexo los productos importantes con elementos digitales. Deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo a fin de identificar los productos con elementos digitales regulados por otras normas de la Unión que supongan el mismo nivel de protección que el presente Reglamento y especificar si sería necesaria una limitación o una exclusión del ámbito de aplicación del presente Reglamento, así como, en su caso, el alcance de dicha limitación. También deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo con respecto a la posible exigencia de certificación ―en el marco de un esquema europeo de certificación― de los productos críticos con elementos digitales que figuran en un anexo del presente Reglamento, así como a la actualización de la lista de productos críticos con elementos digitales, sobre la base de los criterios de criticidad establecidos en el presente Reglamento, y a la especificación de los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que pueden utilizarse para demostrar la conformidad con los requisitos esenciales de ciberseguridad, o partes de ellos, establecidos en un anexo del presente Reglamento. También deben delegarse en la Comisión los poderes para adoptar actos con el fin de especificar el período de soporte mínimo para categorías de producto específicas cuando los datos de vigilancia del mercado indiquen que esos períodos resultan inadecuados, así como de especificar las condiciones de aplicación de los motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de notificaciones sobre vulnerabilidades aprovechadas activamente.

Asimismo, deben delegarse en la Comisión los poderes para adoptar actos con el fin de crear programas voluntarios de certificación de la seguridad para evaluar la conformidad de los productos con elementos digitales que se consideren programas informáticos libres y de código abierto con todos o algunos de los requisitos esenciales de ciberseguridad u otras obligaciones establecidos en el presente Reglamento, así como de especificar el contenido mínimo de la declaración UE de conformidad y de completar los elementos que deben incluirse en la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, incluidas a expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[30]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados. Los poderes para adoptar actos delegados de conformidad con el presente Reglamento deben otorgarse a la Comisión durante un período de cinco años a partir del … [*fecha de entrada en vigor del presente Reglamento*]. La Comisión debe elaborar 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 debe prorrogarse 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.

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

(118) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para: especificar la descripción técnica de las categorías de productos importantes con elementos digitales establecidas en un anexo del presente Reglamento; especificar el formato y los elementos de la SBOM; especificar el formato y el procedimiento para las notificaciones de vulnerabilidades aprovechadas activamente e incidentes graves que repercutan en la seguridad de los productos con elementos digitales presentadas por los fabricantes; establecer especificaciones comunes en relación con los requisitos técnicos que permiten cumplir los requisitos esenciales de ciberseguridad establecidos en un anexo del presente Reglamento; establecer especificaciones técnicas para las etiquetas, los pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales, su período de soporte y mecanismos para promover su uso y sensibilizar al público sobre la seguridad de los productos con elementos digitales; especificar el formulario de documentación simplificado orientado a las necesidades de las microempresas y las pequeñas empresas; y adoptar decisiones sobre medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el correcto funcionamiento del mercado interior. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[31].

(119) Todas las partes que participen en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, con vistas a garantizar la cooperación constructiva y basada en la confianza de las autoridades de vigilancia del mercado en la Unión y a escala nacional.

---

[31] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) A fin de garantizar el cumplimiento efectivo de las obligaciones establecidas en el presente Reglamento, las autoridades de vigilancia del mercado deben estar facultadas para imponer multas administrativas o solicitar su imposición. Por consiguiente, deben establecerse niveles máximos para las multas administrativas que deben prever las legislaciones nacionales en caso de incumplimiento de las obligaciones establecidas en el presente Reglamento. A la hora de decidir la cuantía de la multa administrativa en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación correspondiente y, como mínimo, las establecidas explícitamente en el presente Reglamento, también si el fabricante es una microempresa o una pequeña o mediana empresa, incluida una empresa emergente, y si las mismas u otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador económico por infracciones similares. Tales circunstancias pueden ser agravantes, en situaciones en las que la infracción cometida por el mismo operador económico persista en el territorio de Estados miembros distintos de aquel en el que ya se haya impuesto una multa administrativa, o bien atenuantes, de modo que se garantice que cualquier otra multa administrativa propuesta por otra autoridad de vigilancia del mercado para el mismo operador económico o el mismo tipo de infracción ya toma en consideración, además de otras circunstancias específicas pertinentes, las sanciones impuestas en otros Estados miembros y la cuantía de estas. En todos estos casos, la multa administrativa acumulada que puedan aplicar las autoridades de vigilancia del mercado de varios Estados miembros a un mismo operador económico por el mismo tipo de infracción debe garantizar el respeto del principio de proporcionalidad. Dado que las multas administrativas no se aplican a las microempresas o pequeñas empresas por el incumplimiento del plazo de veinticuatro horas para presentar notificaciones de alerta temprana de vulnerabilidades aprovechadas activamente o incidentes graves que repercutan en la seguridad de un producto con elementos digitales, ni a los administradores de comunidad de programas informáticos de código abierto por ninguna infracción del presente Reglamento, y respetando el principio de que las sanciones deben ser eficaces, proporcionadas y disuasorias, los Estados miembros no deben imponer otros tipos de sanciones de carácter pecuniario a dichas entidades.

(121) Si las multas administrativas se imponen a una persona que no sea una empresa, al valorar la cuantía apropiada de la multa, la autoridad competente debe tener en cuenta el nivel general de ingresos en el Estado miembro, así como la situación económica de la persona. Debe corresponder a los Estados miembros determinar si se debe imponer multas administrativas a las autoridades públicas y en qué medida.

(122) Los Estados miembros deben examinar, teniendo en cuenta las circunstancias nacionales, la posibilidad de utilizar los ingresos procedentes de las sanciones previstas en el presente Reglamento o su equivalente financiero para apoyar las políticas de ciberseguridad y aumentar el nivel de ciberseguridad en la Unión, entre otras cosas, incrementando el número de profesionales cualificados en materia de ciberseguridad, reforzando el desarrollo de capacidades de las microempresas y las pequeñas y medianas empresas y mejorando la sensibilización pública sobre las ciberamenazas.

(123) En sus relaciones con terceros países, la Unión procura fomentar el comercio internacional de productos regulados. Puede aplicarse una amplia variedad de medidas para facilitar el comercio, incluidos varios instrumentos jurídicos, como los acuerdos de reconocimiento mutuo (ARM) bilaterales (intergubernamentales) para la evaluación de la conformidad y el marcado de productos regulados. Los ARM se establecen entre la Unión y los terceros países que poseen un nivel comparable de desarrollo técnico y un enfoque compatible en lo concerniente a la evaluación de la conformidad. Estos acuerdos se basan en la aceptación mutua de los certificados, las marcas de conformidad y los informes de pruebas emitidos por los organismos de evaluación de la conformidad de cualquiera de las partes de manera conforme con la legislación de la otra parte. Actualmente hay ARM vigentes con varios terceros países. Dichos ARM se han celebrado en varios sectores específicos, que pueden variar según los terceros países. Con el fin de facilitar aún más el comercio y reconociendo que las cadenas de suministro de productos con elementos digitales son mundiales, la Unión, de conformidad con el artículo 218 del TFUE, puede celebrar ARM relativos a la evaluación de la conformidad de los productos regulados por el presente Reglamento. La cooperación con los países terceros asociados también es importante para reforzar la ciberresiliencia a escala mundial, ya que, a largo plazo, contribuirá a reforzar el marco de ciberseguridad tanto dentro como fuera de la Unión.

(124) Los consumidores deben poder hacer valer sus derechos en relación con las obligaciones impuestas a los operadores económicos con arreglo al presente Reglamento mediante acciones de representación en virtud de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo[32]. A tal fin, el presente Reglamento debe establecer que la Directiva (UE) 2020/1828 sea aplicable a las acciones de representación relativas a infracciones del presente Reglamento que perjudiquen o puedan perjudicar los intereses colectivos de los consumidores. Por lo tanto, procede modificar el anexo I de dicha Directiva en consecuencia. Corresponde a los Estados miembros garantizar que dicha modificación se refleje en sus medidas de transposición adoptadas en virtud de dicha Directiva, aunque la adopción de medidas nacionales de transposición a este respecto no es una condición para la aplicabilidad de esa Directiva a las acciones de representación citadas. La aplicabilidad de dicha Directiva a las acciones de representación ejercidas en relación con infracciones de las disposiciones del presente Reglamento que perjudiquen o puedan perjudicar los intereses colectivos de los consumidores cometidas por operadores económicos debe comenzar a partir del … [*36 meses después de la fecha de entrada en vigor del presente Reglamento*].

(125) La Comisión debe evaluar y revisar periódicamente el presente Reglamento, en consulta con las partes interesadas pertinentes, en particular para determinar si se precisa alguna modificación a raíz de cambios en la situación social, política, tecnológica o del mercado. El presente Reglamento facilitará el cumplimiento de las obligaciones en materia de seguridad de la cadena de suministro de las entidades que entran en el ámbito de aplicación del Reglamento (UE) 2022/2554 y de la Directiva (UE) 2022/2555 y utilizan productos con elementos digitales. En el marco de la citada revisión periódica, la Comisión debe evaluar los efectos combinados del marco de ciberseguridad de la Unión.

---

[32] 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).

(126) Los operadores económicos deben disponer de tiempo suficiente para adaptarse a los requisitos establecidos en el presente Reglamento. El presente Reglamento debe ser aplicable a partir del … [*treinta y seis meses después de la fecha de la entrada en vigor del presente Reglamento*], a excepción de las obligaciones de información relativas a vulnerabilidades aprovechadas activamente e incidentes graves que repercutan en la seguridad de productos con elementos digitales, que deben ser aplicables a partir del … [*veintiún meses después de la fecha de entrada en vigor del presente Reglamento*] y de las disposiciones relativas a la notificación de los organismos de evaluación de la conformidad, que deben ser aplicables a partir del … [*dieciocho meses después de la fecha de entrada en vigor del presente Reglamento*].

(127) Es importante prestar apoyo en la aplicación del presente Reglamento a las microempresas y a las pequeñas y medianas empresas, incluidas las empresas emergentes, a fin de minimizar los riesgos para la aplicación derivados de la falta de conocimientos y experiencia en el mercado y de facilitar el cumplimiento por parte de los fabricantes de las obligaciones que les impone el presente Reglamento. El programa Europa Digital y otros programas pertinentes de la Unión proporcionan apoyo financiero y técnico que permite a dichas empresas contribuir al crecimiento de la economía de la Unión y al refuerzo del nivel común de ciberseguridad en la Unión. El Centro Europeo de Competencia en Ciberseguridad y los centros nacionales de coordinación, así como los centros europeos de innovación digital creados por la Comisión y los Estados miembros a escala nacional o de la Unión, también podrían apoyar a las empresas y a las organizaciones del sector público y contribuir a la aplicación del presente Reglamento. Dentro de sus respectivas misiones y ámbitos de competencia, podrían prestar apoyo técnico y científico a las microempresas y a las pequeñas y medianas empresas, por ejemplo para actividades de prueba y evaluaciones de la conformidad por parte de terceros. También podrían fomentar el despliegue de herramientas para facilitar la aplicación del presente Reglamento.

(128) Por otra parte, los Estados miembros deben considerar la posibilidad de adoptar medidas complementarias encaminadas a proporcionar orientación y apoyo a las microempresas y a las pequeñas y medianas empresas, como el establecimiento de espacios controlados de pruebas y canales de comunicación específicos. Con el fin de reforzar el nivel de ciberseguridad en la Unión, los Estados miembros también pueden considerar la posibilidad de prestar apoyo para desarrollar capacidades y competencias relacionadas con la ciberseguridad de los productos con elementos digitales, mejorar la ciberresiliencia de los operadores económicos —en particular de las microempresas y las pequeñas y medianas empresas— y fomentar la sensibilización pública sobre la ciberseguridad de los productos con elementos digitales.

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

(130) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[33], emitió su dictamen el 9 de noviembre de 2022[34].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

---

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

[34] DO C 452 de 29.11.2022, p. 23.

Capítulo I
Disposiciones generales

Artículo 1

Objeto

El presente Reglamento establece:

a) normas para la comercialización de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos;

b) requisitos esenciales de ciberseguridad para el diseño, el desarrollo y la fabricación de productos con elementos digitales, así como obligaciones de los operadores económicos en relación con dichos productos en lo que respecta a la ciberseguridad;

c) requisitos esenciales de ciberseguridad para los procesos de gestión de las vulnerabilidades establecidos por los fabricantes a fin de garantizar la ciberseguridad de los productos con elementos digitales durante el tiempo en que se prevea que los productos vayan a utilizarse, así como obligaciones de los operadores económicos en relación con dichos procesos;

d) normas relativas a la vigilancia del mercado, incluida la supervisión, y a la aplicación de los requisitos y las normas a que se refiere el presente artículo.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento es aplicable a los productos con elementos digitales comercializados cuya finalidad prevista o uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

2. El presente Reglamento no es aplicable a los productos con elementos digitales a los que sean aplicables los siguientes actos jurídicos de la Unión:

   a) el Reglamento (UE) 2017/745;

   b) el Reglamento (UE) 2017/746;

   c) el Reglamento (UE) 2019/2144.

3. El presente Reglamento no es aplicable a los productos con elementos digitales que hayan sido certificados de conformidad con el Reglamento (UE) 2018/1139.

4. El presente Reglamento no es aplicable a los equipos que entran en el ámbito de aplicación de la Directiva 2014/90/UE del Parlamento Europeo y del Consejo[35].

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

5. La aplicación del presente Reglamento a los productos con elementos digitales regulados por otras normas de la Unión que establezcan requisitos que aborden la totalidad o parte de los riesgos cubiertos por los requisitos esenciales de ciberseguridad establecidos en el anexo I podrá limitarse o excluirse cuando:

   a) dicha limitación o exclusión sea coherente con el marco regulador general aplicable a dichos productos, y

   b) las normas sectoriales supongan un nivel de protección equivalente o superior al previsto en el presente Reglamento.

   La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 a fin de completar el presente Reglamento especificando si dicha limitación o exclusión es necesaria, los productos y normas afectados y, si procede, el alcance de la limitación.

6. El presente Reglamento no se aplica a las piezas de recambio que se comercialicen para reemplazar componentes idénticos en productos con elementos digitales y que se fabriquen con arreglo a las mismas especificaciones que los componentes a los que están destinadas a sustituir.

7. El presente Reglamento no se aplica a los productos con elementos digitales desarrollados o modificados exclusivamente con fines de seguridad nacional o defensa ni a los productos diseñados específicamente para el tratamiento de información clasificada.

8. Las obligaciones establecidas en el presente Reglamento no implicarán el suministro de información cuya divulgación sea contraria a los intereses esenciales de seguridad nacional, seguridad pública o defensa de los Estados miembros.

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «producto con elementos digitales»: producto consistente en programas informáticos o equipos informáticos y sus soluciones de procesamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado;

2) «tratamiento de datos a distancia»: tratamiento de datos a distancia para el que el programa informático ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad y cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones;

3) «ciberseguridad»: ciberseguridad tal como se define en el artículo 2, punto 1, del Reglamento (UE) 2019/881;

4) «programa informático»: la parte de un sistema electrónico de información consistente en un código informático;

5) «equipo informático»: sistema electrónico de información físico, o partes de este, capaz de tratar, almacenar o transmitir datos digitales;

6) «componente»: programa o equipo informático destinado a su integración en un sistema electrónico de información;

7) «sistema electrónico de información»: sistema, incluidos los aparatos eléctricos o electrónicos, capaz de tratar, almacenar o transmitir datos digitales;

8) «conexión lógica»: representación virtual de una conexión de datos realizada a través de una interfaz de programa informático;

9) «conexión física»: conexión entre sistemas electrónicos de información o componentes realizada por medios físicos, también mediante interfaces eléctricas, ópticas o mecánicas, cables u ondas de radio;

10) «conexión indirecta»: conexión a un dispositivo o red que no tiene lugar directamente, sino como parte de un sistema más amplio que puede conectarse directamente a dicho dispositivo o red;

11) «nodo final»: cualquier dispositivo conectado a una red que sirve de punto de entrada a dicha red;

12) «operador económico»: el fabricante, el representante autorizado, el importador, el distribuidor o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos con elementos digitales o con la comercialización de productos con elementos digitales de conformidad con el presente Reglamento;

13) «fabricante»: persona física o jurídica que desarrolla o fabrica productos con elementos digitales o para quien se diseñan, desarrollan o fabrican productos con elementos digitales, y que los comercializa con su nombre o marca comercial, ya sea de manera remunerada, monetizada o gratuita;

14) «administrador de comunidad de programas informáticos de código abierto»: persona jurídica, distinta de un fabricante, que tiene la finalidad o el objetivo de dar soporte sistemáticamente y de forma sostenida para el desarrollo de productos específicos con elementos digitales que se consideren programas informáticos libres y de código abierto y estén destinados a actividades comerciales, y que garantiza la viabilidad de dichos productos;

15) «representante autorizado»: persona física o jurídica establecida en la Unión que haya recibido un mandato por escrito de un fabricante para actuar en nombre de este en tareas específicas;

16) «importador»: persona física o jurídica establecida en la Unión que introduce en el mercado un producto con elementos digitales que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión;

17) «distribuidor»: persona física o jurídica que forma parte de la cadena de suministro, distinta del fabricante o el importador, que comercializa un producto con elementos digitales en el mercado de la Unión sin influir sobre sus propiedades;

18) «consumidor»: persona física que actúa con fines ajenos a su actividad económica, negocio, oficio o profesión;

19) «microempresas», «pequeñas empresas» y «medianas empresas»: respectivamente, microempresas, pequeñas y medianas empresas tal como se definen en el anexo de la Recomendación 2003/361/CE;

20) «período de soporte»: el período durante el que el fabricante está obligado a garantizar que las vulnerabilidades de un producto con elementos digitales se gestionen eficazmente y de conformidad con los requisitos esenciales de ciberseguridad formulados en el anexo I, parte II;

21) «introducción en el mercado»: la primera comercialización de un producto con elementos digitales en el mercado de la Unión;

22) «comercialización»: el suministro, ya sea remunerado o gratuito, de un producto con elementos digitales para su distribución o utilización en el mercado de la Unión en el curso de una actividad comercial;

23) «finalidad prevista»: el uso para el que un fabricante concibe un producto con elementos digitales, incluido el contexto y las condiciones de uso concretas, según la información facilitada por el fabricante en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica;

24) «uso razonablemente previsible»: uso que no coincide necesariamente con la finalidad prevista indicada por el fabricante en las instrucciones de uso, los materiales y las declaraciones de promoción y venta y la documentación técnica, pero que puede derivarse de un comportamiento humano o de intervenciones e interacciones técnicas razonablemente previsibles;

25) «uso indebido razonablemente previsible»: el uso de un producto con elementos digitales de un modo que no es conforme con su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas razonablemente previsible;

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

27) «evaluación de la conformidad»: el proceso por el que se verifica si se cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I;

28) «organismo de evaluación de la conformidad»: organismo de evaluación de la conformidad tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008;

29) «organismo notificado»: organismo de evaluación de la conformidad designado de conformidad con el artículo 43 y con otra legislación de armonización pertinente de la Unión;

30) «modificación sustancial»: cambio en un producto con elementos digitales tras su introducción en el mercado que afecta al cumplimiento por parte del producto con elementos digitales de los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, o que provoca la modificación de la finalidad prevista para la que se ha evaluado el producto con elementos digitales;

31) «marcado CE»: marcado con el que un fabricante indica que un producto con elementos digitales y los procesos establecidos por el fabricante son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I y otra legislación de armonización de la Unión aplicable que prevea su colocación;

32) «legislación de armonización de la Unión»: la legislación de la Unión enumerada en el anexo I del Reglamento (UE) 2019/1020 y cualquier otra legislación de la Unión que armonice las condiciones para la comercialización de los productos a los que se aplica dicho Reglamento;

33) «autoridad de vigilancia del mercado»: autoridad de vigilancia del mercado tal como se define en el artículo 3, punto 4, del Reglamento (UE) 2019/1020;

34) «norma internacional»: norma internacional tal como se define en el artículo 2, punto 1, letra a), del Reglamento (UE) n.º 1025/2012;

35) «norma europea»: norma europea tal como se define en el artículo 2, punto 1, letra b), del Reglamento (UE) n.º 1025/2012;

36) «norma armonizada»: norma armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012;

37) «riesgo de ciberseguridad»: la posibilidad de pérdida o perturbación causada por un incidente, expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente;

38) «riesgo de ciberseguridad significativo»: riesgo de ciberseguridad debido al cual, sobre la base de sus características técnicas, se puede considerar que existe una alta probabilidad de que se produzca un incidente capaz de acarrear consecuencias negativas graves, también por causar pérdidas o perturbaciones materiales o inmateriales considerables;

39) «nomenclatura de materiales de los programas informáticos»: registro formal que contiene los detalles y las relaciones de la cadena de suministro de los componentes incluidos en los elementos consistentes en programas informáticos de un producto con elementos digitales;

40) «vulnerabilidad»: deficiencia, susceptibilidad o fallo de un producto con elementos digitales que puede ser aprovechada por una ciberamenaza;

41) «vulnerabilidad aprovechable»: vulnerabilidad que puede ser utilizada de manera efectiva por un agente malintencionado en condiciones operativas prácticas;

42) «vulnerabilidad aprovechada activamente»: vulnerabilidad respecto de la cual existen pruebas fiables de que un agente malintencionado la ha aprovechado en un sistema sin autorización del propietario del sistema;

43) «incidente»: incidente tal como se define en el artículo 6, punto 6, de la Directiva (UE) 2022/2555;

44) «incidente que repercute en la seguridad de un producto con elementos digitales»: incidente que afecta o puede afectar negativamente a la capacidad de un producto con elementos digitales para proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos o las funciones;

45) «cuasiincidente»: cuasiincidente tal como se define en el artículo 6, punto 5, de la Directiva (UE) 2022/2555;

46) «ciberamenaza»: ciberamenaza tal como se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;

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

48) «programa informático libre y de código abierto»: programa informático cuyo código fuente se comparte abiertamente y que se ofrece con arreglo a una licencia libre y de código abierto que abarca todos los derechos para que el programa informático sea libremente accesible, utilizable, modificable y redistribuible;

49) «recuperación»: recuperación tal como se define en el artículo 3, punto 22, del Reglamento (UE) 2019/1020;

50) «retirada»: retirada tal como se define en el artículo 3, punto 23, del Reglamento (UE) 2019/1020;

51) «CSIRT designado como coordinador»: CSIRT designado como coordinador en virtud del artículo 12, apartado 1, de la Directiva (UE) 2022/2555.

Artículo 4

Libre circulación

1. Los Estados miembros no impedirán, en relación con las cuestiones reguladas en el presente Reglamento, la comercialización de productos con elementos digitales que sean conformes con el presente Reglamento.

2. Los Estados miembros no impedirán que en ferias, exposiciones, demostraciones o actos similares se presenten o usen productos con elementos digitales que no sean conformes con el presente Reglamento, incluidos sus prototipos, a condición de que el producto se presente con una señal visible que indique claramente que no es conforme con el presente Reglamento y no debe comercializarse hasta que lo sea.

3. Los Estados miembros no impedirán la comercialización de programas informáticos inacabados que no sean conformes con el presente Reglamento, siempre que dichos programas solo se comercialicen durante un período de tiempo limitado, requerido con fines de prueba, con una señal visible que indique claramente que no son conformes con el presente Reglamento y que no se comercializarán con fines distintos de su prueba.

4. El apartado 3 no se aplicará a los componentes de seguridad a que se refiere la legislación de armonización de la Unión distinta del presente Reglamento.

Artículo 5

Contratación pública o uso de productos con elementos digitales

1. El presente Reglamento no impedirá a los Estados miembros someter los productos con elementos digitales a requisitos de ciberseguridad adicionales para la contratación pública o el uso de dichos productos con fines específicos, también cuando dichos productos se contraten o usen con fines de seguridad nacional o defensa, siempre que dichos requisitos sean compatibles con las obligaciones de los Estados miembros establecidas en el Derecho de la Unión y sean necesarios y proporcionados para la consecución de dichos fines.

2. Sin perjuicio de lo dispuesto en las Directivas 2014/24/UE y 2014/25/UE, cuando se contraten productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros se asegurarán de que en el proceso de contratación pública se tenga en cuenta el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I del presente Reglamento, incluida la capacidad de los fabricantes para abordar las vulnerabilidades de manera eficaz.

Artículo 6

Requisitos aplicables a los productos con elementos digitales

Solo se procederá a la comercialización de los productos con elementos digitales si:

a) cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, a condición de que los productos hayan sido instalados de manera adecuada, mantenidos y utilizados para su finalidad prevista o en condiciones que se puedan prever razonablemente y, en su caso, de que se hayan instalado las actualizaciones de seguridad necesarias, y

b) los procesos establecidos por el fabricante cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

Artículo 7

Productos importantes con elementos digitales

1. Los productos con elementos digitales cuya funcionalidad principal sea la de una categoría de productos establecida en el anexo III se considerarán productos importantes con elementos digitales y estarán sujetos a los procedimientos de evaluación de la conformidad a que se refiere el artículo 32, apartados 2 y 3. La integración de un producto con elementos digitales cuya funcionalidad principal sea la de una categoría de productos establecida en el anexo III no hará por sí sola que el producto en el que esté integrado esté sujeto a los procedimientos de evaluación de la conformidad a que se refiere el artículo 32, apartados 2 y 3.

2. Las categorías de productos con elementos digitales a que se refiere el apartado 1 del presente artículo, divididas en las clases I y II establecidas en el anexo III, satisfacen al menos uno de los criterios siguientes:

a) el producto con elementos digitales desempeña principalmente funciones críticas para la ciberseguridad de otros productos, redes o servicios, como la autenticación y el acceso seguros, la prevención y detección de intrusiones, la seguridad de los nodos finales o la protección de las redes;

b) el producto con elementos digitales desempeña una función que entraña un riesgo significativo de efectos adversos en cuanto a su intensidad y su capacidad para perturbar, controlar o dañar un gran número de otros productos, o la salud, la protección o la seguridad de sus usuarios, a través de una manipulación directa (por ejemplo, una función central del sistema, incluidos la gestión de la red, el control de la configuración, la virtualización o el tratamiento de datos personales).

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 a fin de modificar el anexo III para incluir en la lista una nueva categoría en cualquiera de las clases de categorías de productos con elementos digitales y especificar su definición, para trasladar una categoría de productos de una de las clases a la otra o para retirar una categoría de la lista. A la hora de evaluar la necesidad de modificar la lista establecida en el anexo III, la Comisión tendrá en cuenta las funcionalidades relacionadas con la ciberseguridad o la función y el nivel de riesgo de ciberseguridad que plantean los productos con elementos digitales sobre la base de los criterios a que se refiere el apartado 2 del presente artículo.

Los actos delegados a que se refiere el párrafo primero del presente apartado establecerán, cuando proceda, un período transitorio mínimo de doce meses —en particular, cuando se añada una nueva categoría de productos importantes con elementos digitales a las clases I o II establecidas en el anexo III o se traslade una categoría de la clase I a la II— antes de que comiencen a aplicarse los procedimientos de evaluación de la conformidad pertinentes a que se refiere el artículo 32, apartados 2 y 3, a menos que se justifique un período transitorio más breve por razones imperiosas de urgencia.

4. A más tardar el … [*doce meses a partir de la fecha de entrada en vigor del presente Reglamento*], la Comisión adoptará un acto de ejecución que especifique la descripción técnica de las categorías de productos con elementos digitales de las clases I y II establecidas en el anexo III y la descripción técnica de las categorías de productos con elementos digitales establecidas en el anexo IV. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

Artículo 8

Productos críticos con elementos digitales

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 por los que se complete el presente Reglamento a fin de determinar qué productos con elementos digitales cuya funcionalidad básica es la de una categoría de productos establecida en el anexo IV del presente Reglamento deben estar obligados a obtener un certificado europeo de ciberseguridad con un nivel de garantía al menos «sustancial» en el marco de un esquema europeo de certificación de la ciberseguridad adoptado en virtud del Reglamento (UE) 2019/881 para demostrar su conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I del presente Reglamento o partes de ellos, siempre que se haya adoptado un esquema europeo de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 aplicable a esas categorías de productos con elementos digitales y que dicho esquema esté a disposición de los fabricantes. Dichos actos delegados especificarán el nivel de garantía requerido, que será proporcional al nivel de riesgo de ciberseguridad asociado a los productos con elementos digitales y tendrá en cuenta su finalidad prevista, incluida la dependencia crítica respecto de los productos por parte de las entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555.

Antes de adoptar dichos actos delegados, la Comisión llevará a cabo una evaluación de la posible repercusión de las medidas previstas en el mercado y consultará a las partes interesadas pertinentes, incluido el Grupo Europeo de Certificación de la Ciberseguridad establecido en virtud del Reglamento (UE) 2019/881. La evaluación tendrá en cuenta la preparación y el nivel de capacidad de los Estados miembros para la aplicación del correspondiente esquema europeo de certificación de la ciberseguridad. Cuando no se hayan adoptado los actos delegados a que se refiere el párrafo primero del presente apartado, los productos con elementos digitales cuya funcionalidad básica sea la de una categoría de productos establecida en el anexo IV se someterán a los procedimientos de evaluación de la conformidad a que se refiere el artículo 32, apartado 3.

Los actos delegados a que se refiere el párrafo primero establecerán un período transitorio mínimo de seis meses, a menos que se justifique un período transitorio más breve por razones imperiosas de urgencia.

2. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 a fin de modificar el anexo IV añadiendo o suprimiendo categorías de productos críticos con elementos digitales. Al determinar dichas categorías de productos críticos con elementos digitales y el nivel de garantía exigido de conformidad con el apartado 1 del presente artículo, la Comisión tendrá en cuenta los criterios a que se refiere el artículo 7, apartado 2, y se asegurará de que las categorías de productos con elementos digitales cumplen al menos uno de los criterios siguientes:

a) las entidades esenciales a que se refiere el artículo 3 de la Directiva (UE) 2022/2555 presentan una dependencia crítica de la categoría de productos con elementos digitales;

b) los incidentes y las vulnerabilidades aprovechadas que afecten a la categoría de productos con elementos digitales pueden dar lugar a perturbaciones graves de las cadenas de suministro críticas en todo el mercado interior.

Antes de adoptar dichos actos delegados, la Comisión llevará a cabo una evaluación del tipo a que se refiere el apartado 1.

Los actos delegados a que se refiere el párrafo primero establecerán un período transitorio mínimo de seis meses, a menos que se justifique un período transitorio más breve por razones imperiosas de urgencia.

Artículo 9

Consultas con las partes interesadas

1. Al elaborar medidas para la aplicación del presente Reglamento, la Comisión consultará a las partes interesadas pertinentes ―como las autoridades pertinentes de los Estados miembros, las empresas del sector privado, incluidas las microempresas y las pequeñas y medianas empresas, la comunidad de programas informáticos de código abierto, las asociaciones de consumidores, el mundo académico y los órganos y organismos pertinentes de la Unión, así como los grupos de expertos establecidos a escala de la Unión― y tendrá en cuenta sus puntos de vista. En particular, la Comisión, de manera estructurada, cuando proceda, consultará a dichas partes interesadas y recabará sus puntos de vista en los casos siguientes:

   a) al elaborar las orientaciones a que hace referencia el artículo 26;

   b) al elaborar las descripciones técnicas de las categorías de productos establecidas en el anexo III de conformidad con el artículo 7, apartado 4, evaluar la necesidad de posibles actualizaciones de la lista de categorías de productos de conformidad con el artículo 7, apartado 3, y el artículo 8, apartado 2, o llevar a cabo la evaluación de la posible repercusión en el mercado a que se refiere el artículo 8, apartado 1, sin perjuicio de lo dispuesto en el artículo 61;

   c) al llevar a cabo trabajos preparatorios para la evaluación y revisión del presente Reglamento.

2. La Comisión organizará sesiones periódicas de consulta e información, al menos una vez al año, para recabar los puntos de vista de las partes interesadas a que se refiere el apartado 1 sobre la aplicación del presente Reglamento.

Artículo 10

Refuerzo de las competencias en un entorno digital ciberresiliente

A efectos del presente Reglamento, y con el fin de responder a las necesidades de los profesionales en apoyo de la aplicación del presente Reglamento, los Estados miembros, con el apoyo, cuando proceda, de la Comisión, el Centro Europeo de Competencia en Ciberseguridad y la ENISA, y respetando plenamente la responsabilidad de los Estados miembros en el ámbito de la educación, promoverán medidas y estrategias destinadas a:

a) desarrollar competencias en materia de ciberseguridad y crear herramientas organizativas y tecnológicas para garantizar una disponibilidad suficiente de profesionales cualificados con el fin de apoyar las actividades de las autoridades de vigilancia del mercado y los organismos de evaluación de la conformidad;

b) aumentar la colaboración entre el sector privado, los operadores económicos (también mediante la recapacitación y perfeccionamiento profesional de los empleados de los fabricantes), los consumidores, los proveedores de formación y las administraciones públicas, ampliando así las opciones para que las personas jóvenes accedan a un puesto de trabajo en el sector de la ciberseguridad.

Artículo 11

Seguridad general de los productos

No obstante lo dispuesto en el artículo 2, apartado 1, párrafo tercero, letra b), del Reglamento (UE) 2023/988, el capítulo III, sección 1, los capítulos V y VII, y los capítulos IX a XI de dicho Reglamento serán aplicables a los productos con elementos digitales en lo que respecta a los aspectos y los riesgos o categorías de riesgos no contemplados en el presente Reglamento cuando dichos productos no estén obligados a cumplir requisitos de seguridad específicos establecidos en otra «legislación de armonización de la Unión» tal como se define en el artículo 3, punto 27, del Reglamento (UE) 2023/988.

Artículo 12

Sistemas de IA de alto riesgo

1. Sin perjuicio de los requisitos relativos a precisión y solidez establecidos en el artículo 15 del Reglamento (UE) 2024/1689, los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento y estén clasificados como sistemas de IA de alto riesgo en virtud del artículo 6 del Reglamento (UE) 2024/1689 se considerarán conformes con los requisitos relativos a la ciberseguridad establecidos en el artículo 15 de dicho Reglamento cuando:

    a) dichos productos cumplan los requisitos esenciales de ciberseguridad de ciberseguridad establecidos en el anexo I, parte I;

b) los procesos establecidos por el fabricante cumplan los requisitos esenciales de ciberseguridad s de ciberseguridad establecidos en el anexo I, parte II, y

c) la declaración UE de conformidad emitida con arreglo al presente Reglamento demuestre la consecución del nivel de protección de ciberseguridad exigido con arreglo al artículo 15 del Reglamento (UE) 2024/1689.

2. En el caso de los productos con elementos digitales y los requisitos de ciberseguridad mencionados en el apartado 1 del presente artículo será aplicable el procedimiento de evaluación de la conformidad pertinente previsto en el artículo 43 del Reglamento (UE) 2024/1689. A efectos de dicha evaluación, los organismos notificados que sean competentes para controlar la conformidad de los sistemas de IA de alto riesgo en el marco del Reglamento (UE) 2024/1689 también serán competentes para controlar la conformidad de los sistemas de IA de alto riesgo incluidos en el ámbito de aplicación del presente Reglamento con los requisitos establecidos en el anexo I del presente Reglamento, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos dispuestos en el artículo 39 del presente Reglamento en el contexto del procedimiento de notificación previsto en el Reglamento (UE) 2024/1689.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, los productos importantes con elementos digitales enumerados en el anexo III del presente Reglamento sujetos a los procedimientos de evaluación de la conformidad establecidos en el artículo 32, apartado 2, letras a) y b), y apartado 3, del presente Reglamento, así como los productos críticos con elementos digitales enumerados en el anexo IV del presente Reglamento que estén obligados a obtener un certificado de ciberseguridad europeo de conformidad con el artículo 8, apartado 1, del presente Reglamento o, de no ser así, estén sujetos a los procedimientos de evaluación de la conformidad a que se refiere el artículo 32, apartado 3, del presente Reglamento, que además estén clasificados como sistemas de IA de alto riesgo en virtud del artículo 6 del Reglamento (UE) 2024/1689 y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo VI del Reglamento (UE) 2024/1689 estarán sujetos a los procedimientos de evaluación de la conformidad previstos en el presente Reglamento en lo que respecta a los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento.

4. Los fabricantes de productos con elementos digitales a que se refiere el apartado 1 del presente artículo podrán participar en los espacios controlados de pruebas para la IA a que se refiere el artículo 57 del Reglamento (UE) 2024/1689.

Capítulo II
Obligaciones de los operadores económicos y disposiciones relativas a los programas informáticos libres y de código abierto

Artículo 13

Obligaciones de los fabricantes

1. Cuando se introduzca en el mercado un producto con elementos digitales, los fabricantes garantizarán que el producto ha sido diseñado, desarrollado y producido de conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I.

2. A efectos del cumplimiento del apartado 1, los fabricantes llevarán a cabo una evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales y tendrán en cuenta el resultado de dicha evaluación durante las fases de planificación, diseño, desarrollo, producción, entrega y mantenimiento del producto con elementos digitales, con el objetivo de minimizar los riesgos de ciberseguridad, prevenir incidentes y reducir al mínimo sus repercusiones, incluidas las relacionadas con la salud y la seguridad de los usuarios.

3. La evaluación de los riesgos de ciberseguridad se documentará y actualizará según proceda durante un período de soporte que se determinará de conformidad con el apartado 8 del presente artículo. Dicha evaluación de los riesgos de ciberseguridad incluirá, como mínimo, un análisis de los riesgos de ciberseguridad basado en la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales, así como sus condiciones de uso, tales como el entorno operativo o los activos que deben protegerse, teniendo en cuenta el período de tiempo durante el que se prevé que el producto esté en uso. La evaluación de los riesgos de ciberseguridad indicará si los requisitos de seguridad establecidos en el anexo I, parte I, punto 2, son aplicables al producto con elementos digitales en cuestión, y en caso afirmativo de qué manera, así como el modo en que se aplican en la práctica dichos requisitos sobre la base de la evaluación de los riesgos de ciberseguridad. También indicará cómo debe aplicar el fabricante el anexo I, parte I, punto 1, y los requisitos de gestión de las vulnerabilidades establecidos en el anexo I, parte II.

4. Al introducir en el mercado un producto con elementos digitales, el fabricante incluirá la evaluación de riesgos de ciberseguridad a que se refiere el apartado 3 del presente artículo en la documentación técnica exigida en virtud del artículo 31 y el anexo VII. En el caso de los productos con elementos digitales a que se refieren el artículo 12 a los que también se apliquen otros actos jurídicos de la Unión, la evaluación de los riesgos de ciberseguridad podrá formar parte de la evaluación de riesgos exigida por dichos actos jurídicos de la Unión. Cuando determinados requisitos esenciales de ciberseguridad no sean aplicables al producto con elementos digitales, el fabricante incluirá una justificación clara a tal efecto en la documentación técnica citada.

5. A efectos del cumplimiento de lo dispuesto en el apartado 1, los fabricantes ejercerán la diligencia debida al integrar componentes procedentes de terceros de modo que estos componentes no comprometan la seguridad del producto con elementos digitales, también cuando se integren componentes de programas informáticos libres y de código abierto que no se hayan comercializado en el transcurso de una actividad comercial.

6. Cuando los fabricantes detecten una vulnerabilidad en un componente —también de código abierto— integrado en el producto con elementos digitales, notificarán la vulnerabilidad a la persona o entidad que fabrica o mantiene el componente y abordarán y subsanarán la vulnerabilidad de conformidad con los requisitos de gestión de las vulnerabilidades establecidas en el anexo I, parte II. Cuando los fabricantes hayan desarrollado una modificación de un programa o equipo informático para abordar la vulnerabilidad de dicho componente, compartirán el código o la documentación pertinentes con la persona o entidad que fabrica o mantiene el componente, en su caso en un formato legible por máquina.

7. Los fabricantes documentarán sistemáticamente, de manera proporcionada a la naturaleza y a los riesgos de ciberseguridad, los aspectos pertinentes relativos a la ciberseguridad del producto con elementos digitales, incluidas las vulnerabilidades de las que tengan conocimiento y cualquier información pertinente facilitada por terceros, y, cuando corresponda, actualizarán la evaluación de los riesgos de ciberseguridad del producto.

8. Cuando los fabricantes introduzcan en el mercado un producto con elementos digitales, y durante el período de soporte, se asegurarán de que las vulnerabilidades de dicho producto, incluidos sus componentes, se gestionen de manera efectiva y de conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

Los fabricantes determinarán el período de soporte de manera que refleje el período de tiempo durante el cual se prevé que vaya a utilizarse el producto, teniendo en cuenta, en particular, las expectativas razonables de los usuarios, la naturaleza del producto —incluida su finalidad prevista— y el Derecho pertinente de la Unión que fija la vida útil del producto con elementos digitales. A la hora de determinar el período de soporte, los fabricantes también podrán tener en cuenta los períodos de soporte de productos con elementos digitales que ofrezcan una funcionalidad similar introducidos en el mercado por otros fabricantes, la disponibilidad del entorno operativo y los períodos de soporte de los componentes integrados que proporcionan las funciones principales y se obtienen de terceros, así como las orientaciones pertinentes facilitadas por el Grupo de Cooperación Administrativa (ADCO) específico establecido en virtud del artículo 52, apartado 15, y por la Comisión. Las cuestiones que deban tenerse en cuenta para determinar la duración del período de soporte se considerarán de manera que se garantice la proporcionalidad.

Sin perjuicio de lo dispuesto en el párrafo segundo, el período de soporte será de al menos cinco años. Cuando se prevea que el producto con elementos digitales vaya a utilizarse durante menos de cinco años, el período de soporte corresponderá al tiempo de utilización previsto.

Teniendo en cuenta las recomendaciones del ADCO a que se refiere el artículo 52, apartado 16, la Comisión podrá adoptar actos delegados de conformidad con el artículo 61 para completar el presente Reglamento especificando el período de soporte mínimo para determinadas categorías de productos cuando los datos de vigilancia del mercado indiquen que los períodos de soporte son inadecuados.

Los fabricantes incluirán en la documentación técnica establecida en el anexo VII la información que se haya tenido en cuenta para determinar el período de soporte de un producto con elementos digitales.

Los fabricantes contarán con políticas y procedimientos adecuados, incluidas las políticas de divulgación coordinada de vulnerabilidades a que se refiere el anexo I, parte II, punto 5, para tratar y subsanar las posibles vulnerabilidades del producto con elementos digitales comunicadas por fuentes internas o externas.

9. Los fabricantes se asegurarán de que cada una de las actualizaciones de seguridad a que se refiere el anexo I, parte II, punto 8, que se haya puesto a disposición de los usuarios durante el período de soporte siga estando disponible tras su publicación durante un período mínimo de diez años o durante el resto del período de soporte si este plazo fuera más largo.

10. Cuando un fabricante haya introducido en el mercado versiones posteriores modificadas sustancialmente de un producto consistente en un programa informático, podrá garantizar el cumplimiento del requisito esencial de ciberseguridad establecido en el anexo I, parte II, punto 2, únicamente para la versión que haya introducido en el mercado más recientemente siempre que los usuarios de las versiones introducidas con anterioridad en el mercado tengan acceso a la última versión introducida en el mercado de forma gratuita y no incurran en costes adicionales para adaptar el entorno de equipos y programas informáticos en el que utilizan la versión anterior del producto en cuestión.

11. Los fabricantes podrán mantener archivos públicos de programas informáticos que mejoren el acceso de los usuarios a las versiones históricas. En tales casos, se informará claramente y de manera fácilmente accesible a los usuarios sobre los riesgos asociados al uso de programas informáticos a los que no se da soporte.

12. Antes de introducir en el mercado un producto con elementos digitales, los fabricantes elaborarán la documentación técnica especificada en el artículo 31.

    También pondrán en práctica o encargarán que se pongan en práctica los procedimientos de evaluación de la conformidad de su elección a que se refiere el artículo 32.

    Cuando mediante dicho procedimiento de evaluación de la conformidad se haya demostrado la conformidad del producto con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y la conformidad de los procesos establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II, los fabricantes elaborarán la declaración UE de conformidad con arreglo al artículo 28 y colocarán el marcado CE de conformidad con el artículo 30.

13. Los fabricantes mantendrán la documentación técnica y la declaración UE de conformidad a disposición de las autoridades de vigilancia del mercado durante un mínimo de diez años a partir de la introducción en el mercado del producto con elementos digitales, o durante el período de soporte si este plazo fuera más largo.

14. Los fabricantes se asegurarán de que existan procedimientos para que los productos con elementos digitales que formen parte de una producción en serie mantengan su conformidad con el presente Reglamento. Los fabricantes tomarán debidamente en consideración los cambios en el proceso de desarrollo y producción o en el diseño o las características del producto con elementos digitales, así como los cambios en las normas armonizadas, en los esquemas europeos de certificación de la ciberseguridad o en las especificaciones técnicas a que se refiere el artículo 27 en virtud de las cuales se declara o por aplicación de las cuales se verifica la conformidad del producto.

15. Los fabricantes se asegurarán de que sus productos con elementos digitales llevan un número de tipo, lote o serie o cualquier otro elemento que permita su identificación o, cuando esto no sea posible, de que dicha información figura en su embalaje o en un documento que acompañe al producto con elementos digitales.

16. Los fabricantes indicarán su nombre, nombre comercial registrado o marca registrada —así como su dirección postal, su dirección de correo electrónico u otros datos de contacto digitales y, en su caso, el sitio web en el que se les puede contactar— en el producto con elementos digitales, en su embalaje o en un documento que acompañe al producto con elementos digitales. Dicha información también se incluirá en la información y las instrucciones para el usuario que figuran en el anexo II. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios y las autoridades de vigilancia del mercado.

17. A efectos del presente Reglamento, los fabricantes designarán un punto de contacto único que permita a los usuarios comunicarse directa y rápidamente con ellos, también para facilitar la notificación de vulnerabilidades del producto con elementos digitales.

Los fabricantes se asegurarán de que los usuarios puedan identificar fácilmente el punto de contacto único. También incluirán el punto de contacto único en la información y las instrucciones para el usuario que figuran en el anexo II.

El punto de contacto único permitirá a los usuarios elegir los medios de comunicación que prefieran y no limitará dichos medios a herramientas automatizadas.

18. Los fabricantes se asegurarán de que los productos con elementos digitales vayan acompañados de la información y las instrucciones para el usuario especificadas en el anexo II, en papel o en formato electrónico. Dichas instrucciones e información se facilitarán en una lengua fácilmente comprensible para los usuarios y las autoridades de vigilancia del mercado. Serán claras, comprensibles, inteligibles y legibles. Permitirán la instalación, el funcionamiento y el uso seguros de los productos con elementos digitales. Los fabricantes mantendrán la información y las instrucciones para el usuario a que se refiere el anexo II a disposición de los usuarios y de las autoridades de vigilancia del mercado durante un mínimo de diez años a partir de la introducción en el mercado del producto con elementos digitales, o durante el período de soporte si este plazo fuera más largo. Cuando la información y las instrucciones citadas se faciliten en línea, los fabricantes se asegurarán de que sean accesibles y fáciles de usar y permanezcan disponibles en línea durante un mínimo de diez años a partir de la introducción en el mercado del producto con elementos digitales, o durante el período de soporte si este plazo fuera más largo.

19. Los fabricantes se asegurarán de que la fecha final del período de soporte a que se refiere el apartado 8, incluidos al menos el mes y el año, se especifique de manera clara y comprensible en el momento de la compra, de manera fácilmente accesible y, en su caso, en el producto con elementos digitales, en su embalaje o por medios digitales.

Cuando sea técnicamente viable habida cuenta de la naturaleza del producto con elementos digitales, los fabricantes mostrarán una notificación a los usuarios que les informe de que su producto con elementos digitales ha alcanzado el final de su período de soporte.

20. Los fabricantes facilitarán una copia de la declaración UE de conformidad o una declaración UE de conformidad simplificada junto con el producto con elementos digitales. Cuando se facilite una declaración UE de conformidad simplificada, esta contendrá la dirección de internet exacta en la que se pueda acceder a la declaración UE de conformidad íntegra.

21. Desde la introducción en el mercado de un producto con elementos digitales y durante el período de soporte, los fabricantes que sepan o tengan motivos para creer que el producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I adoptarán inmediatamente las medidas correctoras necesarias para poner en conformidad el producto con elementos digitales o los procesos del fabricante, para retirar el producto del mercado o para recuperarlo, según proceda.

22. Previa solicitud motivada de una autoridad de vigilancia del mercado, los fabricantes facilitarán a esa autoridad, bien en papel o bien en formato electrónico y redactadas en una lengua fácilmente comprensible para dicha autoridad, toda la información y documentación necesarias para demostrar la conformidad del producto con elementos digitales y de los procesos establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I. Los fabricantes cooperarán con dicha autoridad, a petición de esta, en cualquier medida que se adopte para eliminar los riesgos de ciberseguridad que presente el producto con elementos digitales que hayan introducido en el mercado.

23. El fabricante que cese sus actividades y, en consecuencia, no pueda cumplir el presente Reglamento informará del próximo cese de las actividades, antes de que dicho cese surta efecto, a las autoridades de vigilancia del mercado pertinentes, así como, por cualquier medio disponible y en la medida de lo posible, a los usuarios de los correspondientes productos con elementos digitales introducidos en el mercado.

24. La Comisión podrá especificar, mediante actos de ejecución que tengan en cuenta las normas y buenas prácticas europeas o internacionales, el formato y los elementos de la nomenclatura de materiales de los programas informáticos a que se refiere el anexo I, parte II, punto 1. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

25. A fin de evaluar la dependencia de los Estados miembros y de la Unión en su conjunto respecto de componentes consistentes en programas informáticos, y en particular respecto de componentes que se consideren programas informáticos libres y de código abierto, el ADCO podrá decidir llevar a cabo en toda la Unión una evaluación de la dependencia correspondiente a categorías concretas de productos con elementos digitales. A tal fin, las autoridades de vigilancia del mercado podrán solicitar a los fabricantes de dichas categorías de productos con elementos digitales que faciliten las correspondientes nomenclaturas de materiales de los programas informáticos a que se refiere el anexo I, parte II, punto 1. Sobre la base de dicha información, las autoridades de vigilancia del mercado podrán facilitar al ADCO información anonimizada y agregada sobre las dependencias en materia de programas informáticos. El ADCO presentará un informe sobre los resultados de la evaluación de la dependencia al Grupo de Cooperación establecido en virtud del artículo 14 de la Directiva (UE) 2022/2555.

Artículo 14

Obligaciones de información de los fabricantes

1. Los fabricantes notificarán simultáneamente al CSIRT designado como coordinador, de conformidad con el apartado 7 del presente artículo, y a la ENISA cualquier vulnerabilidad aprovechada activamente presente en el producto con elementos digitales de la que tengan conocimiento. El fabricante notificará dicha vulnerabilidad aprovechada activamente a través de la plataforma única de notificación establecida en virtud del artículo 16.

2. A efectos de la notificación a que se refiere el apartado 1, el fabricante presentará:

   a) una notificación de alerta temprana de la vulnerabilidad aprovechada activamente, sin demora indebida y, en todo caso, en un plazo de veinticuatro horas desde que el fabricante haya tenido conocimiento de ella, que indique, cuando proceda, los Estados miembros en cuyo territorio el fabricante tenga conocimiento de que se ha comercializado su producto con elementos digitales;

b) a menos que ya se haya facilitado la información pertinente, una notificación de la vulnerabilidad, sin demora indebida y, en todo caso, en un plazo de setenta y dos horas a partir del momento en que el fabricante haya tenido conocimiento de la vulnerabilidad aprovechada activamente, que proporcionará la información general disponible sobre el producto con elementos digitales en cuestión, la naturaleza general de la vulnerabilidad en cuestión y el modo en que es aprovechada, así como sobre las medidas correctoras o paliativas adoptadas y las medidas correctoras o paliativas que los usuarios pueden adoptar, y que también indicará, cuando proceda, en qué medida el fabricante considera sensible la información notificada;

c) a menos que ya se haya facilitado la información pertinente, un informe final, a más tardar catorce días después de que se disponga de una medida correctora o paliativa, que incluya, como mínimo, lo siguiente:

   i) una descripción de la vulnerabilidad, que incluya su gravedad y sus repercusiones,

   ii) cuando se disponga de ella, información relativa a cualquier agente malintencionado que haya aprovechado o esté aprovechando la vulnerabilidad,

   iii) detalles sobre la actualización de seguridad u otras medidas correctoras disponibles para subsanar la vulnerabilidad.

3. Los fabricantes notificarán simultáneamente al CSIRT designado como coordinador, de conformidad con el apartado 7 del presente artículo, y a la ENISA cualquier incidente grave que repercuta en la seguridad de un producto con elementos digitales del que tengan conocimiento. El fabricante notificará dicho incidente a través de la plataforma única de notificación establecida en virtud del artículo 16.

4. A efectos de la notificación a que se refiere el apartado 3, el fabricante presentará:

a) una notificación de alerta temprana del incidente grave que repercute en la seguridad de un producto con elementos digitales, sin demora indebida y, en todo caso, en un plazo de veinticuatro horas desde que el fabricante haya tenido conocimiento de él, que indique como mínimo si se sospecha que el incidente se debe a actos ilegales o malintencionados y que también indicará, cuando proceda, los Estados miembros en cuyo territorio el fabricante tenga conocimiento de que se ha comercializado su producto con elementos digitales;

b) a menos que ya se haya facilitado la información pertinente, una notificación del incidente, sin demora indebida y, en todo caso, en un plazo de setenta y dos horas a partir del momento en que el fabricante haya tenido conocimiento del incidente, que proporcionará la información general disponible sobre la naturaleza del incidente, una evaluación inicial de este, así como información sobre las medidas correctoras o paliativas adoptadas y las medidas correctoras o paliativas que los usuarios pueden adoptar, y que también indicará, cuando proceda, hasta qué punto el fabricante considera sensible la información notificada;

c) a menos que ya se haya facilitado la información pertinente, un informe final, en el plazo de un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, que incluya su gravedad y sus repercusiones,

ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente,

iii) las medidas paliativas aplicadas y en curso.

5. A efectos del apartado 3, un incidente que repercuta en la seguridad de un producto con elementos digitales se considerará grave cuando:

a) afecte o puede afectar negativamente a la capacidad de un producto con elementos digitales para proteger la disponibilidad, autenticidad, integridad o confidencialidad de datos o funciones sensibles o importantes, o

b) haya llevado o pueda llevar a la introducción o ejecución de código malicioso en un producto con elementos digitales o en la red y los sistemas de información de un usuario del producto con elementos digitales.

6. En caso necesario, el CSIRT designado como coordinador que reciba inicialmente la notificación podrá solicitar a los fabricantes que faciliten un informe provisional con actualizaciones pertinentes de la situación relativas a la vulnerabilidad aprovechada activamente o al incidente grave que repercute en la seguridad de un producto con elementos digitales.

7. Las notificaciones a que se refieren los apartados 1 y 3 del presente artículo se presentarán a través de la plataforma única de notificación a que se refiere el artículo 16, utilizando uno de los nodos finales para notificaciones electrónicas a que se refiere el artículo 16, apartado 1. La notificación se presentará utilizando el nodo final para notificaciones electrónicas del CSIRT designado como coordinador del Estado miembro en el que el fabricante tenga su establecimiento principal en la Unión, y será accesible simultáneamente para la ENISA.

A efectos del presente Reglamento, se considerará que el establecimiento principal en la Unión del fabricante se encuentra en el Estado miembro en el que se adopten de forma predominante las decisiones relativas a la ciberseguridad de sus productos con elementos digitales. Si no puede determinarse dicho Estado miembro, se considerará que el establecimiento principal se encuentra en el Estado miembro en el que el fabricante de que se trate tenga el establecimiento con mayor número de trabajadores en la Unión.

Cuando un fabricante no tenga un establecimiento principal en la Unión, presentará las notificaciones a que se refieren los apartados 1 y 3 utilizando el nodo final para notificaciones electrónicas del CSIRT designado como coordinador en el Estado miembro que se determine según la siguiente prelación y sobre la base de la información de que disponga el fabricante:

a) el Estado miembro en el que esté establecido el representante autorizado que actúe en nombre del fabricante para el mayor número de productos con elementos digitales de dicho fabricante;

b) el Estado miembro en el que esté establecido el importador que introduzca en el mercado el mayor número de productos con elementos digitales de dicho fabricante;

c) el Estado miembro en el que esté establecido el distribuidor que comercialice el mayor número de productos con elementos digitales de dicho fabricante;

d) el Estado miembro en el que esté situado el mayor número de usuarios de productos con elementos digitales de dicho fabricante.

En relación con el párrafo tercero, letra d), un fabricante podrá presentar notificaciones relacionadas con cualquier vulnerabilidad posterior aprovechada activamente, o cualquier incidente grave posterior que repercuta en la seguridad de un producto con elementos digitales, al mismo CSIRT designado como coordinador al que haya presentado la primera notificación.

8. Una vez tenga conocimiento de una vulnerabilidad aprovechada activamente o de un incidente grave con repercusiones en la seguridad de un producto con elementos digitales, el fabricante informará a los usuarios afectados del producto con elementos digitales —y, cuando proceda, a todos los usuarios— sobre la dicha vulnerabilidad o incidente y, cuando así se requiera, sobre cualquier reducción de riesgos y las medidas correctoras que los usuarios puedan adoptar para atenuar las repercusiones de la vulnerabilidad o del incidente, en su caso en un formato legible por máquina estructurado que sea fácilmente susceptible de tratamiento automatizado. Cuando el fabricante no informe en el plazo oportuno a los usuarios del producto con elementos digitales, los CSIRT designados como coordinadores que hayan sido notificados podrán facilitar dicha información a los usuarios cuando se considere proporcionado y necesario para prevenir o mitigar las repercusiones de la vulnerabilidad o el incidente en cuestión.

9. A más tardar … [*doce meses después de la fecha de entrada en vigor del presente Reglamento*], la Comisión adoptará actos delegados de conformidad con el artículo 61 del presente Reglamento para completar el presente Reglamento mediante la especificación de las condiciones de aplicación de los motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de notificaciones a que se refiere el artículo 16, apartado 2, del presente Reglamento. La Comisión cooperará con la red de CSIRT establecida en virtud del artículo 15 de la Directiva (UE) 2022/2555 y con la ENISA en la preparación de los proyectos de actos delegados.

10. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de las notificaciones a que se refieren el presente artículo y los artículos 15 y 16. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2. La Comisión cooperará con la red de CSIRT y con la ENISA en la preparación de los proyectos de estos actos de ejecución.

Artículo 15

Notificación voluntaria

1. Los fabricantes, así como otras personas físicas o jurídicas, podrán notificar de forma voluntaria a un CSIRT designado como coordinador o a la ENISA cualquier vulnerabilidad presente en un producto con elementos digitales, así como las ciberamenazas que puedan afectar al perfil de riesgo de un producto con elementos digitales.

2. Los fabricantes, así como otras personas físicas o jurídicas, podrán notificar de forma voluntaria a un CSIRT designado como coordinador o a la ENISA cualquier incidente que repercuta en la seguridad de un producto con elementos digitales, así como los cuasiincidentes que hubieran podido desembocar en un incidente de esas características.

3. El CSIRT designado como coordinador o la ENISA tramitarán las notificaciones a que se refieren los apartados 1 y 2 del presente artículo de conformidad con el procedimiento establecido en el artículo 16.

   El CSIRT designado como coordinador podrá dar prioridad a la tramitación de notificaciones obligatorias sobre la de notificaciones voluntarias.

4. Cuando una persona física o jurídica distinta del fabricante notifique una vulnerabilidad aprovechada activamente o un incidente grave que repercuta en la seguridad de un producto con elementos digitales de conformidad con los apartados 1 o 2, el CSIRT designado como coordinador informará sin demora indebida al fabricante.

5. Los CSIRT designados como coordinadores y la ENISA garantizarán la confidencialidad y la protección adecuada de la información proporcionada por las personas físicas o jurídicas notificantes. Sin perjuicio de la prevención, investigación, detección y enjuiciamiento de infracciones penales, la notificación voluntaria no dará lugar a la imposición a la persona física o jurídica notificante de obligaciones adicionales a las que no estaría sujeta de no haber presentado dicha notificación.

Artículo 16

Creación de una plataforma única de notificación

1. A efectos de las notificaciones a que se refieren el artículo 14, apartados 1 y 3, y el artículo 15, apartados 1 y 2, y con el fin de simplificar las obligaciones de notificación de los fabricantes, la ENISA creará una plataforma única de notificación. La ENISA gestionará y mantendrá las operaciones cotidianas de dicha plataforma única de notificación. La arquitectura de la plataforma única de notificación permitirá a los Estados miembros y a la ENISA establecer sus propios nodos finales para notificaciones electrónicas.

2. Tras recibir una notificación, el CSIRT designado como coordinador que reciba inicialmente la notificación la difundirá sin demora a través de la plataforma única de notificación a los CSIRT designados como coordinadores en cuyo territorio el fabricante haya indicado que se ha comercializado el producto con elementos digitales.

En circunstancias excepcionales y, en particular, a petición del fabricante y debido al grado de sensibilidad de la información notificada indicado por el fabricante con arreglo al artículo 14, apartado 2, letra a), del presente Reglamento, la difusión de la notificación podrá aplazarse durante el período de tiempo estrictamente necesario por motivos justificados relacionados con la ciberseguridad, también cuando una vulnerabilidad esté sujeta al procedimiento de divulgación coordinada de las vulnerabilidades a que se refiere el artículo 12, apartado 1, de la Directiva (UE) 2022/2555. Cuando un CSIRT decida retener una notificación, comunicará inmediatamente dicha decisión a la ENISA y proporcionará tanto una justificación de la retención de la notificación como una indicación de cuándo difundirá la notificación de conformidad con el procedimiento de difusión establecido en el presente apartado. La ENISA podrá prestar apoyo al CSIRT en la aplicación de motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de la notificación.

En circunstancias particularmente excepcionales, cuando el fabricante indique en la notificación a que se refiere el artículo 14, apartado 2, letra b), alguna de las situaciones siguientes:

a) que la vulnerabilidad notificada ha sido aprovechada activamente por un agente malintencionado y que, según la información disponible, no ha sido aprovechada en ningún Estado miembro salvo en el del CSIRT designado como coordinador al que el fabricante ha notificado la vulnerabilidad;

b) que cualquier difusión ulterior inmediata de la vulnerabilidad notificada podría dar lugar al suministro de información cuya divulgación sería contraria a los intereses fundamentales de dicho Estado miembro, o

c) que la vulnerabilidad notificada plantea un elevado riesgo de ciberseguridad inminente derivado de una difusión ulterior;

solo se facilitará simultáneamente a la ENISA, hasta que se difunda la notificación completa a los CSIRT afectados y a la ENISA, la información de que el fabricante ha efectuado una notificación, la información general sobre el producto, la información sobre el carácter general del aprovechamiento de la vulnerabilidad y la información de que se han alegado motivos relacionados con la seguridad. Cuando, sobre la base de la información citada, la ENISA considere que existe un riesgo sistémico que afecta a la seguridad en el mercado interior, recomendará al CSIRT receptor que difunda la notificación completa a los demás CSIRT designados como coordinadores y a la propia ENISA.

3. Tras recibir una notificación de una vulnerabilidad aprovechada activamente en un producto con elementos digitales o de un incidente grave que repercuta en la seguridad de un producto con elementos digitales, los CSIRT designados como coordinadores facilitarán a las autoridades de vigilancia del mercado de sus respectivos Estados miembros la información notificada necesaria para que las autoridades de vigilancia del mercado cumplan sus obligaciones con arreglo al presente Reglamento.

4. La ENISA adoptará medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos para la seguridad de la plataforma única de notificación y la información presentada o difundida a través de la plataforma única de notificación. Notificará sin demora indebida a la red de CSIRT, así como a la Comisión, cualquier incidente de seguridad que afecte a la plataforma única de notificación.

5. La ENISA, en cooperación con la red de CSIRT, proporcionará y aplicará especificaciones sobre las medidas técnicas, operativas y organizativas relativas al establecimiento, el mantenimiento y el funcionamiento seguro de la plataforma única de notificación a que se refiere el apartado 1, que incluyan al menos las disposiciones de seguridad relacionadas con la creación, el funcionamiento y el mantenimiento de la plataforma única de notificación, así como los nodos finales para notificaciones electrónicas establecidos por los CSIRT designados como coordinadores a escala nacional y por la ENISA a escala de la Unión, incluidos aspectos de procedimiento que garanticen que, cuando no se disponga de medidas correctoras o paliativas en relación con una vulnerabilidad notificada, la información sobre dicha vulnerabilidad se comparta conforme a estrictos protocolos de seguridad y sobre la base de la necesidad de conocerla.

6. Cuando una vulnerabilidad aprovechada activamente se haya puesto en conocimiento de un CSIRT designado como coordinador en el marco del procedimiento de divulgación coordinada de vulnerabilidades a que se refiere el artículo 12, apartado 1, de la Directiva (UE) 2022/2555, el CSIRT designado como coordinador que haya recibido inicialmente la notificación podrá aplazar la difusión de la notificación pertinente a través de la plataforma única de notificación por motivos justificados relacionados con la ciberseguridad, durante un período no superior al estrictamente necesario y hasta que las partes involucradas en la divulgación coordinada de vulnerabilidades den su consentimiento. Este requisito no impedirá que los fabricantes notifiquen la vulnerabilidad en cuestión de forma voluntaria de conformidad con el procedimiento establecido en el presente artículo.

Artículo 17

Otras disposiciones relativas a las notificaciones

1. La ENISA podrá presentar a la red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe) creada en virtud del artículo 16 de la Directiva (UE) 2022/2555 la información notificada con arreglo al artículo 14, apartados 1 y 3, y al artículo 15, apartados 1 y 2, del presente Reglamento, si dicha información es pertinente para la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo. A efectos de determinar dicha pertinencia, la ENISA podrá tomar en consideración los análisis técnicos realizados por la red de CSIRT, cuando se disponga de ellos.

2. Cuando sea necesaria la sensibilización del público para prevenir o atenuar un incidente grave que repercuta en la seguridad de un producto con elementos digitales o para gestionar un incidente en curso, o cuando la divulgación del incidente resulte de interés público por otro motivo, el CSIRT designado como coordinador del Estado miembro de que se trate podrá, previa consulta al fabricante afectado y, en su caso, en cooperación con la ENISA, informar al público sobre el incidente o exigir al fabricante que lo haga.

3. Sobre la base de las notificaciones recibidas en virtud del artículo 14, apartados 1 y 3, y al artículo 15, apartados 1 y 2, del presente Reglamento, la ENISA elaborará cada veinticuatro meses un informe técnico sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en los productos con elementos digitales y lo presentará al Grupo de Cooperación creado en virtud del artículo 14 de la Directiva (UE) 2022/2555. El primero de estos informes se presentará en un plazo de veinticuatro meses a partir de la fecha en que empiecen a ser aplicables las obligaciones establecidas en el artículo 14, apartados 1 y 3. La ENISA incluirá información pertinente de sus informes técnicos en su informe sobre la situación de ciberseguridad en la Unión con arreglo al artículo 18 de la Directiva (UE) 2022/2555.

4. El mero acto de notificación de conformidad con el artículo 14, apartados 1 y 3, o el artículo 15, apartados 1 y 2, no entrañará un incremento de la responsabilidad para la persona física o jurídica notificante.

5. Una vez que se disponga de una actualización de seguridad u otra forma de medida correctora o paliativa, la ENISA, de acuerdo con el fabricante del producto con elementos digitales de que se trate, incorporará la vulnerabilidad conocida públicamente notificada en virtud del artículo 14, apartado 1, o al artículo 15, apartado 1, del presente Reglamento a la base de datos europea de vulnerabilidades creada en virtud del artículo 12, apartado 2, de la Directiva (UE) 2022/2555.

6. Los CSIRT designados como coordinadores prestarán apoyo en calidad de servicio de asistencia en relación con las obligaciones de notificación en virtud del artículo 14 a los fabricantes y, en particular, a los fabricantes que se consideren microempresas o pequeñas o medianas empresas.

Artículo 18

Representantes autorizados

1. El fabricante podrá designar a un representante autorizado mediante mandato escrito.

2. Las obligaciones establecidas en el artículo 13, apartados 1 a 11, apartado 12, párrafo primero, y apartado 14 no formarán parte del mandato del representante autorizado.

3. El representante autorizado efectuará las tareas especificadas en el mandato recibido del fabricante. El representante autorizado proporcionará copia del mandato a las autoridades de vigilancia del mercado a petición de estas. El mandato permitirá al representante autorizado realizar como mínimo las tareas siguientes:

a) mantener la declaración UE de conformidad a que se refiere el artículo 28 y la documentación técnica a que se refiere el artículo 31 a disposición de las autoridades de vigilancia del mercado durante un mínimo de diez años a partir de la introducción en el mercado del producto con elementos digitales, o durante el período de soporte si este plazo fuera más largo;

b) en respuesta a una solicitud motivada de una autoridad de vigilancia del mercado, facilitar a dicha autoridad toda la información y documentación necesarias para demostrar la conformidad del producto con elementos digitales;

c) cooperar con las autoridades de vigilancia del mercado, a petición de estas, en cualquier acción destinada a eliminar los riesgos planteados por un producto con elementos digitales objeto del mandato del representante autorizado.

Artículo 19

Obligaciones de los importadores

1. Los importadores solo introducirán en el mercado productos con elementos digitales que cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y siempre que los procesos establecidos por el fabricante cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

2. Antes de introducir en el mercado un producto con elementos digitales, los importadores se asegurarán de que:

   a) el fabricante ha llevado a cabo los procedimientos de evaluación de la conformidad adecuados a que se refiere el artículo 32;

   b) el fabricante ha redactado la documentación técnica;

   c) el producto con elementos digitales lleva el marcado CE contemplado en el artículo 30 y va acompañado de la declaración UE de conformidad a que se refiere el artículo 13, apartado 20, y de la información y las instrucciones para el usuario especificadas en el anexo II, en una lengua fácilmente comprensible para los usuarios y las autoridades de vigilancia del mercado;

   d) el fabricante ha cumplido los requisitos establecidos en el artículo 13, apartados 15, 16 y 19.

   A efectos del presente apartado, los importadores deberán estar en condiciones de presentar los documentos necesarios que demuestren el cumplimiento de los requisitos establecidos en el presente artículo.

3. Si un importador considera o tiene motivos para creer que un producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con el presente Reglamento, no introducirá el producto en el mercado hasta que el producto o los procesos establecidos por el fabricante no se hayan puesto en conformidad con el presente Reglamento. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, el importador informará de ello al fabricante y a las autoridades de vigilancia del mercado.

Cuando un importador tenga motivos para creer, que un producto con elementos digitales puede entrañar un riesgo de ciberseguridad significativo debido a factores de riesgo no técnicos, informará de ello a las autoridades de vigilancia del mercado. Tras recibir dicha información, las autoridades de vigilancia del mercado seguirán los procedimientos a que se refiere el artículo 54, apartado 2.

4. Los importadores indicarán su nombre, nombre comercial registrado o marca registrada, su dirección postal, su dirección de correo electrónico u otros datos de contacto digitales y, en su caso, el sitio web en el que se les puede contactar en el producto con elementos digitales, en su embalaje o en un documento que acompañe al producto con elementos digitales. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios finales y las autoridades de vigilancia del mercado.

5. Los importadores que sepan o tengan motivos para creer que un producto con elementos digitales que han introducido en el mercado no es conforme con el presente Reglamento adoptarán inmediatamente las medidas correctoras necesarias para garantizar que dicho producto con elementos digitales se ponga en conformidad con el presente Reglamento, o bien para retirarlo del mercado o recuperarlo, cuando proceda.

   Cuando tengan conocimiento de una vulnerabilidad en el producto con elementos digitales, los importadores informarán al fabricante sobre dicha vulnerabilidad sin demora indebida. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, los importadores informarán inmediatamente de ello a las autoridades de vigilancia del mercado de los Estados miembros en los que lo hayan comercializado y proporcionarán detalles, en particular, sobre la no conformidad y sobre cualquier medida correctora adoptada.

6. Durante un período mínimo de diez años a partir de la introducción del producto con elementos digitales en el mercado, o durante el período de soporte si este plazo fuera más largo, los importadores conservarán una copia de la declaración UE de conformidad a disposición de las autoridades de vigilancia del mercado y se asegurarán de que, previa petición, dichas autoridades puedan disponer de la documentación técnica.

7. Previa solicitud motivada de una autoridad de vigilancia del mercado, los importadores facilitarán a esta, bien en papel o bien en formato electrónico y redactadas en una lengua fácilmente comprensible para dicha autoridad, toda la información y documentación necesarias para demostrar la conformidad del producto con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, así como la conformidad de los procesos establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II. Cooperarán con dicha autoridad, a petición de esta, en cualquier medida adoptada para eliminar los riesgos de ciberseguridad que presente el producto con elementos digitales que hayan introducido en el mercado.

8. Cuando el importador de un producto con elementos digitales tenga conocimiento de que el fabricante de dicho producto ha cesado sus actividades y, en consecuencia, no puede cumplir las obligaciones establecidas en el presente Reglamento, el importador informará de esa situación a las autoridades de vigilancia del mercado pertinentes, así como, por cualquier medio disponible y en la medida de lo posible, a los usuarios de los correspondientes productos con elementos digitales introducidos en el mercado.

Artículo 20

Obligaciones de los distribuidores

1. Al comercializar un producto con elementos digitales, los distribuidores actuarán con la diligencia debida en relación con los requisitos establecidos en el presente Reglamento.

2. Antes de comercializar un producto con elementos digitales, los distribuidores comprobarán que:

a) el producto con elementos digitales lleva el marcado CE;

b) el fabricante y el importador han cumplido las obligaciones establecidas, respectivamente, en el artículo 13, apartados 15, 16, 18, 19 y 20, y en el artículo 19, apartado 4, y han facilitado todos los documentos necesarios al distribuidor.

3. Si un distribuidor considera o tiene motivos para creer, con arreglo a la información que obre en su poder, que un producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I, el distribuidor no comercializará el producto con elementos digitales hasta que el producto o los procesos establecidos por el fabricante no se hayan puesto en conformidad con el presente Reglamento. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, el distribuidor informará de ello sin demora indebida al fabricante y a las autoridades de vigilancia del mercado.

4. Los distribuidores que sepan o tengan motivos para creer, con arreglo a la información que obre en su poder, que un producto con elementos digitales que han comercializado o los procesos establecidos por su fabricante no son conformes con el presente Reglamento se asegurarán de que se adopten las medidas correctoras necesarias para poner en conformidad dicho producto con elementos digitales o los procesos establecidos por su fabricante, o bien para retirar el producto del mercado o recuperarlo, cuando proceda.

Cuando tengan conocimiento de una vulnerabilidad en el producto con elementos digitales, los distribuidores informarán al fabricante sobre dicha vulnerabilidad sin demora indebida. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, los distribuidores informarán inmediatamente de ello a las autoridades de vigilancia del mercado de los Estados miembros en los que lo hayan comercializado y proporcionarán detalles, en particular, sobre la no conformidad y sobre cualquier medida correctora adoptada.

5. Previa solicitud motivada de una autoridad de vigilancia del mercado, los distribuidores facilitarán a esta, bien en papel o bien en formato electrónico y redactadas en una lengua fácilmente comprensible para dicha autoridad, toda la información y documentación necesarias para demostrar la conformidad del producto con elementos digitales y de los procesos establecidos por el fabricante con el presente Reglamento. Cooperarán con dicha autoridad, a petición de esta, en cualquier medida adoptada para eliminar los riesgos de ciberseguridad planteadas por el producto con elementos digitales que han comercializado.

6. Cuando el distribuidor de un producto con elementos digitales tenga conocimiento, con arreglo a la información que obre en su poder, de que el fabricante ha cesado sus actividades y, en consecuencia, no puede cumplir las obligaciones establecidas en el presente Reglamento, el distribuidor informará sin demora de esa situación a las autoridades de vigilancia del mercado pertinentes, así como, por cualquier medio disponible y en la medida de lo posible, a los usuarios de los correspondientes productos con elementos digitales introducidos en el mercado.

Artículo 21

Casos en que las obligaciones de los fabricantes son aplicables a los importadores y distribuidores

A los efectos del presente Reglamento, se considerará fabricante a un importador o distribuidor, a quien, por consiguiente, se le aplicará lo dispuesto en los artículos 13 y 14, cuando dicho importador o distribuidor introduzca en el mercado un producto con elementos digitales con su nombre o marca o lleve a cabo una modificación sustancial de un producto con elementos digitales que ya se haya introducido en el mercado.

Artículo 22

Otros casos en que son aplicables las obligaciones de los fabricantes

1. A los efectos del presente Reglamento, se considerará fabricante a una persona física o jurídica, distinta del fabricante, el importador o el distribuidor, que lleve a cabo una modificación sustancial de un producto con elementos digitales y comercialice dicho producto.

2. La persona a que se refiere el apartado 1 del presente artículo deberá cumplir las obligaciones establecidas en los artículos 13 y 14 con respecto a la parte del producto con elementos digitales afectada por la modificación sustancial o, si la modificación sustancial afecta a la ciberseguridad del producto con elementos digitales en su conjunto, con respecto a la totalidad del producto.

Artículo 23

Identificación de los operadores económicos

1. Previa solicitud, los operadores económicos facilitarán la siguiente información a las autoridades de vigilancia del mercado:

   a) el nombre y la dirección de cualquier operador económico que les haya suministrado un producto con elementos digitales;

   b) cuando dispongan de ellos, el nombre y la dirección de cualquier operador económico al que hayan suministrado un producto con elementos digitales.

2. Los operadores económicos deberán estar en condiciones de aportar la información a que se refiere el apartado 1 durante diez años a partir de que se les haya suministrado el producto con elementos digitales y durante diez años a partir de que ellos hayan suministrado el producto con elementos digitales.

Artículo 24

Obligaciones de los administradores de comunidad de programas informáticos de código abierto

1. Los administradores de comunidad de programas informáticos de código abierto establecerán y documentarán de manera verificable una política de ciberseguridad para fomentar el desarrollo de un producto con elementos digitales seguro, así como una gestión eficaz de las vulnerabilidades por parte de los desarrolladores de dicho producto. Dicha política también fomentará la notificación voluntaria de vulnerabilidades, tal como se establece en el artículo 15, por parte de los desarrolladores de dicho producto, y tendrá en cuenta la naturaleza específica del administrador de comunidad de programas informáticos de código abierto y las disposiciones jurídicas y organizativas a las que esté sujeto. La política incluirá, en particular, aspectos relacionados con la documentación de las vulnerabilidades, la respuesta a ellas y su subsanación, y promoverá el intercambio de información sobre las vulnerabilidades descubiertas en la comunidad de código abierto.

2. Los administradores de comunidad de programas informáticos de código abierto cooperarán con las autoridades de vigilancia del mercado, a petición de estas, con vistas a reducir los riesgos de ciberseguridad planteados por productos con elementos digitales que se consideren programas informáticos libres y de código abierto.

   Previa solicitud motivada de una autoridad de vigilancia del mercado, los administradores de comunidad de programas informáticos de código abierto facilitarán a dicha autoridad, en una lengua fácilmente comprensible para esta, la documentación a que se refiere el apartado 1, en papel o en formato electrónico.

3. Las obligaciones establecidas en el artículo 14, apartado 1, se aplicarán a los administradores de comunidad de programas informáticos de código abierto en la medida en que participen en el desarrollo de los productos con elementos digitales. Las obligaciones establecidas en el artículo 14, apartados 3 y 8, se aplicarán a los administradores de comunidad de programas informáticos de código abierto en la medida en que un incidente grave que repercuta en la seguridad de productos con elementos digitales afecte a las redes y a los sistemas de información proporcionados por los administradores de comunidad de programas informáticos de código abierto para el desarrollo de los productos en cuestión.

Artículo 25

Certificación de seguridad de los programas informáticos libres y de código abierto

A fin de facilitar el cumplimiento de la obligación de diligencia debida establecida en el artículo 13, apartado 5, en particular en lo que respecta a los fabricantes que integren en sus productos con elementos digitales componentes consistentes en programas informáticos libres y de código abierto, la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 por los que se complete el presente Reglamento estableciendo programas voluntarios de certificación de seguridad que permitan a los desarrolladores o usuarios de productos con elementos digitales que se consideren programas informáticos libres y de código abierto, así como a otros terceros, evaluar la conformidad de dichos productos con todos o algunos de los requisitos esenciales de ciberseguridad u otras obligaciones establecidos en el presente Reglamento.

Artículo 26

Orientaciones

1. A fin de facilitar la ejecución y garantizar que esta sea coherente, la Comisión publicará orientaciones para ayudar a los operadores económicos a aplicar el presente Reglamento, haciendo especial hincapié en facilitar su cumplimiento por parte de las microempresas y pequeñas y medianas empresas.

2. Cuando se proponga proporcionar las orientaciones a que se refiere el apartado 1, la Comisión abordará al menos los siguientes aspectos:

   a) el ámbito de aplicación del presente Reglamento, haciendo especial hincapié en las soluciones de tratamiento de datos a distancia y los programas informáticos libres y de código abierto;

   b) la aplicación de períodos de soporte en relación con determinadas categorías de productos con elementos digitales;

   c) orientaciones dirigidas a fabricantes a los que se aplica el presente Reglamento a los que también se aplica la legislación de armonización de la Unión distinta del presente Reglamento o a otros actos jurídicos conexos de la Unión;

   d) el concepto de modificación sustancial.

   La Comisión también mantendrá una lista de fácil acceso con los actos delegados y de ejecución adoptados en virtud del presente Reglamento.

3. A la hora de elaborar las orientaciones previstas en el presente artículo, la Comisión consultará a las partes interesadas pertinentes.

Capítulo III
Conformidad del producto con elementos digitales

Artículo 27

Presunción de conformidad

1. Se presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante que sean conformes con normas armonizadas o partes de estas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I que estén regulados por dichas normas o partes de ellas.

   La Comisión, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, solicitará a uno o varios organismos europeos de normalización que elaboren normas armonizadas para los requisitos esenciales de ciberseguridad que se establecen en el anexo I al presente Reglamento. Al prepararlas solicitudes de normalización para el presente Reglamento, la Comisión procurará tener en cuenta las normas europeas e internacionales en materia de ciberseguridad que estén vigentes o en curso de desarrollo con el fin de simplificar el desarrollo de las normas armonizadas, de conformidad con el Reglamento (UE) n.º 1025/2012.

2. La Comisión estará facultada para adoptar actos de ejecución por los que se establezcan especificaciones comunes relativas a los requisitos técnicos que proporcionen un medio para cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I para los productos con componentes digitales incluidos en el ámbito de aplicación del presente Reglamento.

Dichos actos de ejecución solo se adoptarán cuando se cumplan las condiciones siguientes:

a) que, en virtud de lo dispuesto en el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, la Comisión haya solicitado que una o varias organizaciones europeas de normalización elaboren una norma armonizada relativa a los requisitos esenciales de ciberseguridad establecidos en el anexo I y que:

i) la solicitud no haya sido aceptada,

ii) las normas armonizadas que respondan a esa solicitud no se hayan 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 no se ajusten a la solicitud, y

b) que no se haya publicado en el *Diario Oficial de la Unión Europea* ninguna referencia a normas armonizadas que regulen los requisitos esenciales de ciberseguridad pertinentes establecidos en el anexo I de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevea la publicación de ninguna referencia en un plazo razonable.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

3. Antes de preparar el proyecto de acto delegado a que se refiere el apartado 2 del presente artículo, 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 2.

4. Al preparar el proyecto de acto de ejecución a que se refiere el apartado 2, la Comisión tendrá en cuenta los puntos de vista de los organismos pertinentes y consultará debidamente a todas las partes interesadas pertinentes.

5. Se presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante que sean conformes con las especificaciones comunes establecidas por los actos de ejecución a que hace referencia el apartado 2 del presente artículo, o partes de estas, son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I a que se refieran dichas especificaciones comunes o partes de estas.

6. Cuando un organismo europeo de normalización adopte una norma armonizada y la proponga 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 se publique la referencia de una norma armonizada en el *Diario Oficial de la Unión Europea*, la Comisión derogará los actos de ejecución a que se refiere el apartado 2, o las partes de estos que se refieran a los mismos requisitos esenciales de ciberseguridad regulados que sean objeto de dicha norma armonizada.

7. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos esenciales de ciberseguridad establecidos en el anexo I, informará de ello a la Comisión presentando una explicación detallada. La Comisión evaluará dicha explicación detallada y podrá modificar, si procede, el acto de ejecución por el que se hubiera establecido la especificación común en cuestión.

8. Se presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante para los que se haya expedido una declaración UE de conformidad o un certificado en el marco de un esquema europeo de certificación de la ciberseguridad adoptado en virtud del Reglamento (UE) 2019/881 son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I en la medida en que la declaración UE de conformidad o el certificado europeo de ciberseguridad, o partes de ellos, abarquen dichos requisitos.

9. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 61 del presente Reglamento a fin de completar el presente Reglamento mediante la especificación de los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que puedan servir para demostrar la conformidad de los productos con elementos digitales con los requisitos esenciales de ciberseguridad, o partes de ellos, establecidos en el anexo I. Asimismo, la expedición de un certificado de ciberseguridad europeo en el marco de dichos esquemas, con un nivel de garantía como mínimo «sustancial», elimina la obligación de un fabricante de llevar a cabo una evaluación de la conformidad por parte de terceros para los requisitos correspondientes, tal como se establece en el artículo 32, apartado 2, letras a) y b), y apartado 3, letras a) y b), del presente Reglamento.

Artículo 28

Declaración UE de conformidad

1. La declaración UE de conformidad será elaborada por los fabricantes con arreglo a lo dispuesto en el artículo 13, apartado 12, y hará constar que se ha demostrado el cumplimiento de los requisitos esenciales de ciberseguridad aplicables establecidos en el anexo I.

2. La declaración UE de conformidad tendrá la estructura tipo establecida en el anexo V y contendrá los elementos especificados en los procedimientos de evaluación de la conformidad correspondientes establecidos en el anexo VIII. La declaración se mantendrá actualizada como corresponda. Estará disponible en la lengua o las lenguas requeridas por el Estado miembro donde se introduzca en el mercado o se comercialice el producto con elementos digitales.

La declaración UE de conformidad simplificada a que se refiere el artículo 13, apartado 20, se ajustará al modelo establecido en el anexo VI. Estará disponible en la lengua o las lenguas requeridas por el Estado miembro donde se introduzca en el mercado o se comercialice el producto con elementos digitales.

3. Cuando un producto con elementos digitales esté sometido a más de un acto jurídico de la Unión que exija una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos esos actos jurídicos de la Unión. Dicha declaración contendrá la identificación de los actos jurídicos de la Unión correspondientes y sus referencias de publicación.

4. Al elaborar una declaración UE de conformidad, el fabricante asumirá la responsabilidad de la conformidad del producto con elementos digitales.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 a fin de completar el presente Reglamento añadiendo elementos al contenido mínimo de la declaración UE de conformidad establecido en el anexo V a fin de tener en cuenta los avances tecnológicos.

Artículo 29

Principios generales del marcado CE

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

Artículo 30

Reglas y condiciones para la colocación del marcado CE

1. El marcado CE se colocará en el producto con elementos digitales de manera visible, legible e indeleble. Cuando ello no sea posible o no se justifique dada la naturaleza del producto con elementos digitales, se colocará en el embalaje y en la declaración UE de conformidad mencionada en el artículo 28 que acompañen al producto con elementos digitales. En el caso de los productos con elementos digitales en forma de programas informáticos, el marcado CE se colocará en la declaración UE de conformidad mencionada en el artículo 28 o el sitio web que acompañen al producto. En este último caso, los consumidores deberán poder acceder de manera sencilla y directa al apartado pertinente del sitio web.

2. Habida cuenta de la naturaleza del producto con elementos digitales, la altura del marcado CE colocado en él podrá ser inferior a 5 mm, siempre y cuando siga siendo visible y legible.

3. El marcado CE se colocará antes de que el producto con elementos digitales se introduzca en el mercado. Podrá ir seguido de un pictograma o cualquier otra marca que indique un riesgo o uso de ciberseguridad especiales establecidos en los actos de ejecución a que se refiere el apartado 6.

4. El marcado CE irá seguido del número de identificación del organismo notificado cuando dicho organismo participe en el procedimiento de evaluación de la conformidad basado en el aseguramiento de calidad total (basado en el módulo H) a que hace referencia el artículo 32.

Dicho número de identificación del organismo notificado será colocado por el propio organismo notificado o bien, siguiendo las instrucciones de este, por el fabricante o por el representante autorizado de este.

5. Los Estados miembros se basarán en los mecanismos existentes para garantizar la correcta aplicación del régimen que regula el marcado CE y adoptarán las medidas adecuadas en caso de uso indebido de dicho marcado. Cuando al producto con elementos digitales se aplique otra legislación de armonización de la Unión distinta del presente Reglamento que también requiera la colocación del marcado CE, el marcado CE indicará que el producto también cumple los requisitos establecidos en esa otra legislación de armonización de la Unión.

6. La Comisión podrá, mediante actos de ejecución, establecer especificaciones técnicas para etiquetas, pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales, sus períodos de soporte, así como mecanismos para promover su uso y fomentar la sensibilización pública respecto a la seguridad de los productos con elementos digitales. Al preparar los proyectos de actos de ejecución, la Comisión consultará a las partes interesadas pertinentes y, si ya se ha creado de conformidad con el artículo 52, apartado 15, al ADCO. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

Artículo 31

Documentación técnica

1. La documentación técnica contendrá todos los datos o detalles pertinentes relativos a los medios utilizados por el fabricante para garantizar que el producto con elementos digitales y los procesos establecidos por el fabricante cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I. Incluirá, como mínimo, los elementos establecidos en el anexo VII.

2. La documentación técnica se elaborará antes de que el producto con elementos digitales se introduzca en el mercado y, en su caso, se mantendrá permanentemente actualizada al menos durante el período de soporte.

3. En el caso de los productos con elementos digitales a que se refiere el artículo 12 a los que también se apliquen otros actos jurídicos de la Unión que prevean documentación técnica, se elaborará una única documentación técnica que contenga la información a que hace referencia el anexo VII del presente Reglamento y la información requerida por esos otros actos jurídicos de la Unión.

4. La documentación técnica y la correspondencia relacionada con cualquiera de los procedimientos de evaluación de la conformidad se redactarán en una lengua oficial del Estado miembro en el que esté establecido el organismo notificado, o en una lengua aceptable para este último.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 61 a fin de completar el presente Reglamento mediante la incorporación de elementos que deban figurar en la documentación técnica establecida en el anexo VII a fin de tener en cuenta los avances tecnológicos, así como los imprevistos que surjan durante el proceso de ejecución del presente Reglamento. A tal fin, la Comisión procurará garantizar que la carga administrativa para las microempresas y pequeñas y medianas empresas sea proporcionada.

Artículo 32

Procedimientos de evaluación de la conformidad de los productos con elementos digitales

1. El fabricante llevará a cabo una evaluación de la conformidad del producto con elementos digitales y de los procesos establecidos por el fabricante para determinar si se cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I. El fabricante demostrará la conformidad con los requisitos esenciales de ciberseguridad mediante cualquiera de los procedimientos siguientes:

   a) el procedimiento de control interno (basado en el módulo A) que se establece en el anexo VIII;

   b) el procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VIII, seguido de la conformidad de tipo UE basada en el control interno de la producción (basada en el módulo C) que se establece en el anexo VIII;

c) la evaluación de la conformidad basada en el aseguramiento de calidad total (basada en el módulo H) que se establece en el anexo VIII, o

d) cuando exista y sea aplicable, un esquema europeo de certificación de la ciberseguridad, en virtud del artículo 27, apartado 9.

2. Cuando, al evaluar la conformidad del producto importante con elementos digitales de la clase I según lo establecido en el anexo III y de los procesos establecidos por su fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, el fabricante no haya aplicado o solo haya aplicado parcialmente las normas armonizadas, las especificaciones comunes o los esquemas europeos de certificación de la ciberseguridad a un nivel de garantía como mínimo «sustancial» a que se refiere el artículo 27, o bien cuando no existan tales normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad, la conformidad del producto con elementos digitales de que se trate y de los procesos establecidos por el fabricante respecto de dichos requisitos esenciales de ciberseguridad se evaluará con arreglo a uno de los procedimientos siguientes:

a) procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VIII, seguido de la conformidad de tipo UE basada en el control interno de la producción (basada en el módulo C) que se establece en el anexo VIII, o

b) evaluación de la conformidad basada en el aseguramiento de calidad total (basada en el módulo H) que se establece en el anexo VIII.

3. Cuando el producto sea un producto importante con elementos digitales perteneciente a la clase II según lo establecido en el anexo III, el fabricante demostrará la conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I mediante cualquiera de los procedimientos siguientes:

a) procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VIII, seguido de la conformidad de tipo UE basada en el control interno de la producción (basada en el módulo C) que se establece en el anexo VIII;

b) evaluación de la conformidad basada en el aseguramiento de calidad total (basada en el módulo H) que se establece en el anexo VIII, o

c) cuando esté disponible y sea aplicable, un esquema europeo de certificación de la ciberseguridad con arreglo al artículo 27, apartado 9, del presente Reglamento a un nivel de garantía como mínimo «sustancial» con arreglo al Reglamento (UE) 2019/881.

4. Los productos críticos con elementos digitales que figuran en el anexo IV demostrarán la conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I mediante uno de los procedimientos siguientes:

a) un esquema europeo de certificación de la ciberseguridad de conformidad con el artículo 8, apartado 1, o

b) cuando no se cumplan las condiciones del artículo 8, apartado 1, cualquiera de los procedimientos a que se refiere el apartado 3 del presente artículo.

5. Los fabricantes de productos con elementos digitales que se consideren programas informáticos libres y de código abierto que entren en las categorías establecidas en el anexo III demostrarán la conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I utilizando uno de los procedimientos a que se refiere el apartado 1 del presente artículo, siempre que la documentación técnica a que se refiere el artículo 31 se ponga a disposición del público en el momento de la introducción en el mercado de esos productos.

6. Se tendrán en cuenta los intereses y necesidades específicos de las microempresas y las pequeñas y medianas empresas, incluidas las empresas emergentes, a la hora de fijar las tarifas que se aplican a los procedimientos de evaluación de la conformidad y se reducirán dichas tarifas de forma proporcionada a dichos intereses y necesidades específicos.

Artículo 33

Medidas de apoyo a las microempresas y las pequeñas y medianas empresas, incluidas las empresas emergentes

1. Los Estados miembros emprenderán, cuando proceda, las siguientes acciones, adaptadas a las necesidades de las microempresas y las pequeñas empresas:

   a) organizar actividades específicas de sensibilización y formación sobre la aplicación del presente Reglamento;

b) establecer un canal específico de comunicación con las microempresas y las pequeñas empresas y, en su caso, con las autoridades públicas locales, para asesorar y responder a las preguntas sobre la aplicación del presente Reglamento;

c) apoyar las actividades de prueba y evaluación de la conformidad, también, cuando proceda, con el apoyo del Centro Europeo de Competencia en Ciberseguridad.

2. Los Estados miembros podrán, cuando proceda, establecer espacios controlados de pruebas de ciberresiliencia. Estos espacios controlados de pruebas ofrecerán entornos de prueba controlados para productos innovadores con elementos digitales a fin de facilitar su desarrollo, diseño, validación y prueba a efectos del cumplimiento del presente Reglamento durante un período de tiempo limitado antes de la introducción en el mercado. La Comisión y, cuando proceda, la ENISA podrán proporcionar apoyo técnico, asesoramiento y herramientas para la creación y el funcionamiento de espacios controlados de pruebas. Los espacios controlados de pruebas se crearán bajo la supervisión, la orientación y el apoyo directos de las autoridades de vigilancia del mercado. Los Estados miembros informarán a la Comisión y a las demás autoridades de vigilancia del mercado del establecimiento de un espacio controlado de pruebas mediante el ADCO. Los espacios controlados de pruebas no afectarán a las facultades de supervisión y correctoras de las autoridades competentes. Los Estados miembros garantizarán un acceso abierto, justo y transparente a los espacios controlados de pruebas y, en particular, facilitarán el acceso de las microempresas y las pequeñas empresas, incluidas las empresas emergentes.

3. De conformidad con el artículo 26, la Comisión proporcionará orientaciones a las microempresas y a las pequeñas y medianas empresas en relación con la aplicación del presente Reglamento.

4. La Comisión informará del apoyo financiero disponible en el marco normativo de los programas de la Unión existentes, en particular a fin de aliviar la carga financiera para las microempresas y pequeñas empresas.

5. Las microempresas y las pequeñas empresas podrán facilitar todos los elementos de la documentación técnica especificada en el anexo VII utilizando un formato simplificado. A tal fin, la Comisión especificará, mediante actos de ejecución, el formulario simplificado de documentación técnica dirigido a las necesidades de las microempresas y las pequeñas empresas, incluida la forma en que deben facilitarse los elementos establecidos en el anexo VII. Cuando una microempresa o pequeña empresa opte por facilitar la información establecida en el anexo VII 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.

   Esos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

Artículo 34

Acuerdos de reconocimiento mutuo

Teniendo en cuenta el nivel de desarrollo técnico y el enfoque de evaluación de la conformidad de un tercer país, la Unión podrá celebrar acuerdos de reconocimiento mutuo con terceros países, de conformidad con el artículo 218 del TFUE, con el fin de promover y facilitar el comercio internacional.

Capítulo IV

Notificación de los organismos de evaluación de la conformidad

Artículo 35

Notificación

1. Los Estados miembros notificarán a la Comisión y a los demás Estados miembros los organismos autorizados a realizar evaluaciones de la conformidad con arreglo al presente Reglamento.

2. Los Estados se esforzarán por garantizar, a más tardar el … [*veinticuatro meses desde la fecha de entrada en vigor del presente Reglamento*], que haya un número suficiente de organismos notificados en la Unión para llevar a cabo evaluaciones de la conformidad, con objeto de evitar cuellos de botella y obstáculos para el acceso al mercado.

Artículo 36

Autoridades notificantes

1. Cada Estado miembro designará una autoridad notificante que será responsable de establecer y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad y para su supervisión, lo que incluye el cumplimiento del artículo 41.

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

3. Cuando la autoridad notificante delegue o encomiende de otro modo la evaluación, la notificación o la supervisión contempladas en el apartado 1 del presente artículo a un organismo que no sea un ente público, dicho organismo será una persona jurídica y cumplirá, *mutatis mutandis*, el artículo 37. Además, este organismo deberá contar con las disposiciones pertinentes para asumir las responsabilidades derivadas de sus actividades.

4. La autoridad notificante asumirá la plena responsabilidad de las tareas realizadas por el organismo mencionado en el apartado 3.

Artículo 37

Requisitos relativos a las autoridades notificantes

1. La autoridad notificante se establecerá de forma que no exista ningún conflicto de intereses con los organismos de evaluación de la conformidad.

2. La autoridad notificante se organizará y funcionará de manera que se preserve la objetividad e imparcialidad de sus actividades.

3. La autoridad notificante se organizará de forma que toda decisión relativa a la notificación de un organismo de evaluación de la conformidad sea adoptada por personas competentes distintas de las que llevaron a cabo la evaluación.

4. La autoridad notificante no ofrecerá ni realizará para terceros ninguna actividad que lleven a cabo los organismos de evaluación de la conformidad, ni servicios de consultoría con carácter comercial o competitivo.

5. La autoridad notificante preservará la confidencialidad de la información obtenida.

6. La autoridad notificante dispondrá de suficiente personal competente para llevar a cabo adecuadamente sus tareas.

Artículo 38

Obligación de información de las autoridades notificantes

1. Los Estados miembros informarán a la Comisión de sus procedimientos de evaluación y notificación de organismos de evaluación de la conformidad y de supervisión de los organismos notificados, así como de cualquier cambio en estos.

2. La Comisión hará pública la información a que se refiere el apartado 1.

Artículo 39

Requisitos relativos a los organismos notificados

1. A efectos de la notificación, los organismos de evaluación de la conformidad cumplirán los requisitos establecidos en los apartados 2 a 12.

2. Los organismos de evaluación de la conformidad se establecerán con arreglo al Derecho nacional y tendrán personalidad jurídica.

3. Los organismos de evaluación de la conformidad serán terceros organismos independientes de la organización o el producto con elementos digitales que evalúen.

   Se puede considerar terceros organismos independientes a los organismos pertenecientes a una asociación comercial o una federación profesional que represente a empresas que participan en el diseño, el desarrollo, la producción, el suministro, el montaje, el uso o el mantenimiento de los productos con elementos digitales que evalúen, a condición de que se demuestre su independencia y la ausencia de conflictos de interés.

4. El organismo de evaluación de la conformidad, sus directivos de alto rango y el personal responsable de la realización de las tareas de evaluación de la conformidad no serán el diseñador, el desarrollador, el fabricante, el proveedor, el importador, el distribuidor, el instalador, el comprador, el dueño, el usuario o el encargado del mantenimiento de los productos con elementos digitales que deben evaluarse, ni el representante autorizado de ninguno de ellos. Ello no impide que usen los productos evaluados que sean necesarios para el funcionamiento del organismo de evaluación de la conformidad, ni para que usen dichos productos con fines personales.

Los organismos de evaluación de la conformidad, sus directivos de alto rango y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la producción, la importación, la distribución, la comercialización, la instalación, el uso ni el mantenimiento de los productos con elementos digitales que evalúan, ni representarán a las partes que participen en estas actividades. No realizarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que hayan sido notificados. Ello se aplicará, en particular, a los servicios de consultoría.

Los organismos de evaluación de la conformidad se asegurarán de que las actividades de sus filiales o subcontratistas no afecten a la confidencialidad, objetividad o imparcialidad de sus actividades de evaluación de la conformidad.

5. Los organismos de evaluación de la conformidad y su personal llevarán a cabo las actividades de evaluación de la conformidad con el máximo nivel de integridad profesional y con la competencia técnica exigida para el campo específico, y estarán libres de cualquier presión o incentivo, especialmente de índole financiera, que pudieran influir en su apreciación o en el resultado de sus actividades de evaluación de la conformidad, en particular por parte de personas o grupos de personas que tengan algún interés en los resultados de estas actividades.

6. El organismo de evaluación de la conformidad será capaz de realizar todas las tareas de evaluación de la conformidad especificadas en el anexo VIII y para las que haya sido notificado, independientemente de si realiza las tareas el propio organismo o si se realizan en su nombre y bajo su responsabilidad.

   En todo momento, para cada procedimiento de evaluación de la conformidad y para cada tipo o categoría de productos con elementos digitales para los que ha sido notificado, el organismo de evaluación de la conformidad dispondrá:

   a) de personal con conocimientos técnicos y experiencia suficiente y adecuada para realizar las tareas de evaluación de la conformidad;

   b) de las descripciones de los procedimientos con arreglo a los cuales se efectuará la evaluación de la conformidad, garantizando la transparencia y la posibilidad de reproducción de estos procedimientos; dispondrá también de las políticas y procedimientos adecuados que diferencien las tareas efectuadas como organismo notificado de otras actividades;

c) de procedimientos para la realización de sus actividades teniendo debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura, el grado de complejidad de la tecnología del producto y el carácter masivo o en serie del proceso de producción.

Los organismos de evaluación de la conformidad dispondrán de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrán acceso a todo el equipo o las instalaciones que necesiten.

7. El personal encargado de llevar a cabo las tareas de evaluación de la conformidad dispondrá de:

a) una buena formación técnica y profesional para realizar todas las actividades de evaluación de la conformidad para las que el organismo de evaluación de la conformidad haya sido notificado;

b) un conocimiento satisfactorio de los requisitos de las evaluaciones que efectúe y la autoridad necesaria para efectuarlas;

c) un conocimiento y una comprensión adecuados de los requisitos esenciales de ciberseguridad establecidos en el anexo I, de las normas armonizadas aplicables y especificaciones comunes, y de las disposiciones pertinentes de la legislación de armonización de la Unión aplicable, así como de los actos de ejecución correspondientes;

d) la capacidad necesaria para elaborar certificados, documentos e informes que demuestren que se han efectuado las evaluaciones.

8. Se garantizará la imparcialidad de los organismos de evaluación de la conformidad, de sus directivos de alto rango y del personal de evaluación.

La remuneración de los directivos de alto rango y del personal de evaluación de los organismos de evaluación de la conformidad no dependerá del número de evaluaciones realizadas ni de los resultados de dichas evaluaciones.

9. El organismo de evaluación de la conformidad suscribirá un seguro de responsabilidad, salvo que su Estado miembro asuma la responsabilidad con arreglo al Derecho interno, o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

10. El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información recabada en el ejercicio de sus tareas, con arreglo al anexo VIII o a cualquier disposición de Derecho interno por la que se aplique, salvo con respecto a las autoridades de vigilancia del mercado del Estado miembro en que realice sus actividades. Se protegerán los derechos de propiedad. El organismo de evaluación de la conformidad contará con procedimientos documentados que garanticen el cumplimiento del presente apartado.

11. Los organismos de evaluación de la conformidad participarán en las actividades pertinentes de normalización y las actividades del grupo de coordinación de los organismos notificados establecido con arreglo al artículo 51, o se asegurarán de que su personal de evaluación esté informado al respecto, y aplicarán a modo de orientaciones generales las decisiones y los documentos administrativos que resulten de las labores del grupo.

12. Los organismos de evaluación de la conformidad funcionarán con arreglo a un conjunto de condiciones coherentes, justas, proporcionadas y razonables, evitando al mismo tiempo cargas innecesarias para los operadores económicos, que tengan particularmente en cuenta los intereses de las microempresas y las pequeñas y medianas empresas en cuanto a las tarifas.

Artículo 40

Presunción de conformidad de los organismos notificados

Si un organismo de evaluación de la conformidad demuestra su conformidad con los criterios establecidos en las normas armonizadas pertinentes, o partes de ellas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, se presumirá que cumple los requisitos establecidos en el artículo 39 en la medida en que las normas armonizadas aplicables cubran estos requisitos.

Artículo 41

Subcontrataciones y filiales de los organismos notificados

1. Cuando un organismo notificado subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplen los requisitos establecidos en el artículo 39 e informará a la autoridad notificante en consecuencia.

2. El organismo notificado asumirá la plena responsabilidad de las tareas realizadas por los subcontratistas o las filiales, con independencia de dónde estén establecidos.

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

4. Los organismos notificados mantendrán a disposición de la autoridad notificante los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial, así como sobre el trabajo que estos realicen con arreglo al presente Reglamento.

Artículo 42

Solicitud de notificación

1. El organismo de evaluación de la conformidad presentará una solicitud de notificación a la autoridad notificante del Estado miembro en el que esté establecido.

2. Dicha solicitud irá acompañada de una descripción de las actividades de evaluación de la conformidad, del procedimiento o procedimientos de evaluación de la conformidad y del producto o productos con elementos digitales para los cuales el organismo se considere competente, así como, cuando proceda, de un certificado de acreditación expedido por un organismo nacional de acreditación, en el que se declare que el organismo de evaluación de la conformidad cumple los requisitos establecidos en el artículo 39.

3. Si el organismo de evaluación de la conformidad en cuestión no puede facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para verificar, reconocer y supervisar regularmente que cumple los requisitos establecidos en el artículo 39.

Artículo 43

Procedimiento de notificación

1. Las autoridades notificantes solo presentarán notificaciones a los organismos de evaluación de la conformidad que hayan satisfecho los requisitos establecidos en el artículo 39.

2. La autoridad notificante pertinente presentará una notificación a la Comisión y a los demás Estados miembros por medio del Sistema de información sobre organismos notificados y designados de nuevo enfoque desarrollado y gestionado por la Comisión.

3. La notificación incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o los módulos de evaluación de la conformidad, el producto o los productos con elementos digitales afectados y la correspondiente certificación de competencia.

4. Si la notificación no está basada en el certificado de acreditación a que se refiere el artículo 42, apartado 2, la autoridad notificante transmitirá a la Comisión y a los demás Estados miembros las pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones existentes destinadas a garantizar que se controlará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 39.

5. El organismo en cuestión solo podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no han formulado ninguna objeción en el plazo de dos semanas a partir de la notificación en caso de que se utilice un certificado de acreditación o de dos meses a partir de la notificación en caso de no se utilice la acreditación.

   Solo entonces ese organismo será considerado un organismo notificado a efectos del presente Reglamento.

6. La Comisión y los demás Estados miembros serán informados de todo cambio pertinente posterior a la notificación.

Artículo 44

Números de identificación y listas de organismos notificados

1. La Comisión asignará un número de identificación a cada organismo notificado.

   Asignará un solo número incluso si el organismo es notificado con arreglo a varios actos jurídicos de la Unión.

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, junto con los números de identificación que les hayan sido asignados y las actividades para las que hayan sido notificados.

   La Comisión se asegurará de que la lista se mantiene actualizada.

Artículo 45

Cambios en las notificaciones

1. Cuando una autoridad notificante compruebe que un organismo notificado ya no cumple los requisitos establecidos en el artículo 39 o no está cumpliendo sus obligaciones, o sea informada de ello, dicha autoridad notificante restringirá, suspenderá o retirará la notificación, según proceda, dependiendo de la gravedad del incumplimiento de los requisitos u obligaciones. Informará inmediatamente a la Comisión y a los demás Estados miembros al respecto.

2. En caso de restricción, suspensión o retirada de la notificación o si el organismo notificado ha cesado en su actividad, el Estado miembro notificante adoptará las medidas oportunas para garantizar que los expedientes de dicho organismo sean tratados por otro organismo notificado o se pongan a disposición de las autoridades notificantes y de vigilancia del mercado responsables cuando estas los soliciten.

Artículo 46

Cuestionamiento de la competencia de los organismos notificados

1. La Comisión investigará todos los casos en los que tenga o le planteen dudas de que un organismo notificado sea competente o cumpla de manera continuada los requisitos y las responsabilidades que deba cumplir.

2. El Estado miembro notificante facilitará a la Comisión, a petición de esta, toda la información en que se base la notificación o el mantenimiento de la competencia del organismo en cuestión.

3. La Comisión garantizará el tratamiento confidencial de toda la información sensible recabada en el curso de sus investigaciones.

4. Cuando la Comisión compruebe que un organismo notificado no cumple o ha dejado de cumplir los requisitos de su notificación, informará al Estado miembro notificante al respecto y le pedirá que adopte las medidas correctoras necesarias, que pueden consistir, si es necesario, en la anulación de la notificación.

Artículo 47

Obligaciones operativas de los organismos notificados

1. Los organismos notificados realizarán evaluaciones de la conformidad de acuerdo con los procedimientos de evaluación de la conformidad establecidos en el artículo 32 y en el anexo VIII.

2. Las evaluaciones de la conformidad se llevarán a cabo de manera proporcionada, evitando imponer cargas innecesarias a los operadores económicos. Los organismos de evaluación de la conformidad llevarán a cabo sus actividades teniendo debidamente en cuenta el tamaño de las empresas, en particular por lo que respecta a las microempresas y a las pequeñas y medianas empresas, el sector en que operan, su estructura, su grado de complejidad y el nivel de riesgo de ciberseguridad del producto con elementos digitales y de la tecnología de que se trate y del carácter masivo o en serie del proceso de producción.

3. Los organismos notificados respetarán, sin embargo, el grado de rigor y el nivel de protección requeridos para que los productos con elementos digitales sean conformes con lo dispuesto en el presente Reglamento.

4. Si un organismo notificado determina que el fabricante no cumple los requisitos establecidos en el anexo I, en las normas armonizadas correspondientes o en las especificaciones comunes a que se refiere el artículo 27, instará al fabricante a adoptar las medidas correctoras oportunas y no expedirá el certificado de conformidad.

5. Si durante la supervisión de la conformidad posterior a la expedición del certificado, un organismo notificado determina que el producto con elementos digitales ya no es conforme con los requisitos establecidos en el presente Reglamento, instará al fabricante a adoptar las medidas correctoras adecuadas y, si es necesario, suspenderá o retirará el certificado.

6. Si no se adoptan medidas correctoras o estas no surten el efecto requerido, el organismo notificado restringirá, suspenderá o retirará cualquier certificado, según corresponda.

Artículo 48

Recurso frente las decisiones de los organismos notificados

Los Estados miembros garantizarán que exista un procedimiento de recurso frente a las decisiones de los organismos notificados.

Artículo 49

Obligación de información de los organismos notificados

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

   a) toda denegación, restricción, suspensión o retirada de un certificado;

   b) toda circunstancia que afecte al ámbito y a las condiciones de notificación;

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

d) previa solicitud, toda actividad de evaluación de la conformidad realizada dentro del ámbito de su notificación y cualquier otra actividad llevada a cabo, con inclusión de la subcontratación y las actividades transfronterizas.

2. Los organismos notificados proporcionarán a los demás organismos notificados con arreglo al presente Reglamento que realicen actividades de evaluación de la conformidad similares con respecto a los mismos productos con elementos digitales información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de la evaluación de la conformidad.

Artículo 50

Intercambio de experiencias

La Comisión dispondrá que se organice el intercambio de experiencias entre las autoridades nacionales de los Estados miembros responsables de la política de notificación.

Artículo 51

Coordinación de los organismos notificados

1. La Comisión se asegurará de que se establezcan y se gestionen convenientemente una coordinación y una cooperación adecuadas entre los organismos notificados, a través de un grupo intersectorial de organismos notificados.

2. Los Estados miembros se asegurarán de que los organismos notificados por ellos participan en el trabajo de dicho grupo, directamente o por medio de representantes designados.

Capítulo V

Vigilancia del mercado y aplicación de la legislación

Artículo 52

Vigilancia del mercado y control de los productos con elementos digitales en el mercado de la Unión

1. El Reglamento (UE) 2019/1020 será aplicable a los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento.

2. Cada Estado miembro designará una o varias autoridades de vigilancia del mercado con el fin de garantizar la aplicación efectiva del presente Reglamento. Los Estados miembros podrán designar una autoridad existente o nueva para que actúe en calidad de autoridad de vigilancia del mercado a efectos del presente Reglamento.

3. Las autoridades de vigilancia del mercado designadas con arreglo al apartado 2 del presente artículo también serán responsables de llevar a cabo actividades de vigilancia del mercado en relación con las obligaciones de los administradores de comunidad de programas informáticos de código abierto establecidas en el artículo 24. Cuando una autoridad de vigilancia del mercado constate que un administrador de comunidad de programas informáticos de código abierto no cumple las obligaciones establecidas en dicho artículo, le exigirá que garantice que se adoptan todas las medidas correctoras adecuadas. Los administradores de comunidad de programas informáticos de código abierto se asegurarán de que se adopten todas las medidas correctoras adecuadas en relación con sus obligaciones en virtud del presente Reglamento.

4. Cuando corresponda, las autoridades de vigilancia del mercado cooperarán con las autoridades nacionales de certificación de la ciberseguridad designadas en virtud del artículo 58 del Reglamento (UE) 2019/881 e intercambiarán información periódicamente. Por lo que respecta a la supervisión de la aplicación de las obligaciones de información en virtud del artículo 14 del presente Reglamento, las autoridades de vigilancia del mercado designadas cooperarán e intercambiarán información de manera periódica con los CSIRT designados como coordinadores y la ENISA.

5. Las autoridades de vigilancia del mercado podrán solicitar a un CSIRT designado como coordinador o a la ENISA asesoramiento técnico sobre cuestiones relacionadas con la aplicación y ejecución del presente Reglamento. Al llevar a cabo una investigación con arreglo al artículo 54, las autoridades de vigilancia del mercado podrán solicitar a un CSIRT designado como coordinador o a la ENISA que proporcione un análisis para apoyar las evaluaciones no vinculantes del cumplimiento de los productos con elementos digitales.

6. Cuando corresponda, las autoridades de vigilancia del mercado cooperarán con otras autoridades de vigilancia del mercado designadas sobre la base de la legislación de armonización de la Unión distinta del presente Reglamento e intercambiarán información periódicamente.

7. Las autoridades de vigilancia del mercado cooperarán, en su caso, con las autoridades responsables de supervisar el Derecho de la Unión en materia de protección de datos. Dicha cooperación implica informar a esas autoridades de toda constatación pertinente para el ejercicio de sus competencias, también al proporcionar orientaciones y asesoramiento en virtud del apartado 10, si dichas orientaciones y asesoramiento se refieren al tratamiento de datos personales.

   Las autoridades responsables de supervisar el Derecho de la Unión en materia de protección de datos estarán facultadas para solicitar cualquier documentación creada o conservada con arreglo al presente Reglamento y acceder a ella cuando el acceso a dicha documentación sea necesario para el ejercicio de sus funciones. Informarán de ello a las autoridades de vigilancia del mercado designadas del Estado miembro pertinente para la solicitud.

8. Los Estados miembros garantizarán que las autoridades de vigilancia del mercado designadas dispongan de recursos financieros y técnicos adecuados, incluidas, cuando proceda, herramientas de automatización del procesamiento, y de recursos humanos con las capacidades necesarias en materia de ciberseguridad para el desempeño de sus funciones con arreglo al presente Reglamento.

9. La Comisión fomentará y facilitará el intercambio de experiencias entre las autoridades de vigilancia del mercado designadas.

10. Las autoridades de vigilancia del mercado, con el apoyo de la Comisión y, cuando proceda, de los CSIRT y la ENISA, podrán proporcionar orientación y asesoramiento a los operadores económicos sobre la aplicación del presente Reglamento.

11. Las autoridades de vigilancia del mercado informarán a los consumidores de dónde presentar reclamaciones que podrían indicar el incumplimiento del presente Reglamento, de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, y facilitarán información a los consumidores sobre dónde y cómo acceder a mecanismos para facilitar la notificación de vulnerabilidades, incidentes y ciberamenazas que puedan afectar a productos con elementos digitales.

12. Las autoridades de vigilancia del mercado facilitarán, cuando proceda, la cooperación con las partes interesadas pertinentes, incluidas las organizaciones científicas, de investigación y de consumidores.

13. Las autoridades de vigilancia del mercado presentarán a la Comisión un informe anual acerca de las actividades pertinentes de vigilancia del mercado. Las autoridades de vigilancia del mercado designadas comunicarán sin demora a la Comisión y a las autoridades nacionales de competencia pertinentes cualquier información recabada durante las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación de las disposiciones del Derecho de la Unión en materia de competencia.

14. En el caso de los productos con elementos digitales que entran en el ámbito de aplicación del presente Reglamento clasificados como sistemas de IA de alto riesgo en virtud del artículo 6 del Reglamento (UE) 2024/1689, las autoridades de vigilancia del mercado designadas a efectos del Reglamento (UE) 2024/1689 serán las autoridades responsables de las actividades de vigilancia del mercado que se requieran en virtud del presente Reglamento. Las autoridades de vigilancia del mercado designadas en virtud del Reglamento (UE) 2024/1689 cooperarán, según proceda, con las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento y, en lo que respecta a la supervisión del cumplimiento de las obligaciones de información que establece el artículo 14 del presente Reglamento, con los CSIRT designados como coordinadores y la ENISA. Las autoridades de vigilancia del mercado designadas en virtud del Reglamento (UE) 2024/1689 informarán, en particular, a las autoridades de vigilancia del mercado designadas en virtud del presente Reglamento de toda constatación pertinente para el ejercicio de sus funciones en relación con la aplicación del presente Reglamento.

15. Se establecerá un ADCO específico para la aplicación uniforme del presente Reglamento, en virtud del artículo 30, apartado 2, del Reglamento (UE) 2019/1020. El ADCO estará compuesto por representantes de las autoridades de vigilancia del mercado designadas y, en su caso, por representantes de las oficinas de enlace únicas. El ADCO también abordará cuestiones específicas relacionadas con las actividades de vigilancia del mercado en relación con las obligaciones impuestas a los administradores de comunidad de programas informáticos de código abierto.

16. Las autoridades de vigilancia del mercado supervisarán cómo los fabricantes han aplicado los criterios a que se refiere el artículo 13, apartado 8, a la hora de determinar el período de soporte de sus productos con elementos digitales.

El ADCO publicará en un formato accesible al público y de fácil uso estadísticas pertinentes sobre las categorías de productos con elementos digitales, incluido su período de soporte medio, según determine el fabricante en virtud del artículo 13, apartado 8, y proporcionará orientaciones que incluyan períodos de soporte indicativos para las categorías de productos con elementos digitales.

Cuando los datos sugieran períodos de soporte inadecuados para categorías específicas de productos con elementos digitales, el ADCO podrá formular recomendaciones a las autoridades de vigilancia del mercado para que centren sus actividades en dichas categorías de productos con elementos digitales.

Artículo 53

Acceso a datos y documentación

Cuando sea necesario para evaluar la conformidad de los productos con elementos digitales y los procesos establecidos por los fabricantes con los requisitos esenciales de ciberseguridad establecidos en el anexo I, se concederá a las autoridades de vigilancia del mercado, previa solicitud motivada, acceso a los datos, en una lengua que les sea fácilmente inteligible, necesarios para evaluar el diseño, el desarrollo y la producción de dichos productos y la gestión de sus vulnerabilidades, incluida la documentación interna correspondiente del operador económico correspondiente.

Artículo 54

Procedimiento a nivel nacional aplicable a los productos con elementos digitales que presentan un riesgo de ciberseguridad significativo

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga un motivo suficiente para considerar que un producto con elementos digitales, también en lo que respecta a la gestión de las vulnerabilidades, presenta un riesgo de ciberseguridad significativo, efectuará, sin demora indebida y en cooperación el CSIRT correspondiente, una evaluación del producto con elementos digitales de que se trate para verificar su cumplimiento de todos los requisitos establecidos en el presente Reglamento. Los operadores económicos pertinentes cooperarán con la autoridad de vigilancia del mercado en todo lo necesario.

Si, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado constata que el producto con elementos digitales no cumple los requisitos establecidos en el presente Reglamento, pedirá sin demora al operador económico pertinente que adopte las medidas correctoras oportunas para llevar el producto con elementos digitales a conformidad con los citados requisitos o bien retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo de ciberseguridad, que la autoridad de vigilancia del mercado prescriba.

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

2. Al determinar la importancia de un riesgo de ciberseguridad a que se refiere el apartado 1 del presente artículo, las autoridades de vigilancia del mercado también tendrán en cuenta los factores de riesgo no técnicos, en particular los establecidos como resultado de las evaluaciones coordinadas de riesgos para la seguridad de las cadenas de suministro críticas a escala de la Unión realizadas de conformidad con el artículo 22 de la Directiva (UE) 2022/2555. Cuando una autoridad de vigilancia del mercado posea motivos suficientes para considerar que un producto con elementos digitales presenta un riesgo de ciberseguridad significativo a la luz de factores de riesgo no técnicos, informará a las autoridades competentes designadas o establecidas en virtud del artículo 8 de la Directiva (UE) 2022/2555 y cooperará con esas autoridades cuando sea necesario.

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 de los resultados de la evaluación y de las medidas que haya instado al operador económico a adoptar.

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

5. Si el operador económico no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 1, párrafo segundo, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del producto con elementos digitales en su mercado nacional, para retirarlo de ese mercado o para recuperarlo.

   Dicha autoridad notificará sin demora a la Comisión y a los demás Estados miembros estas medidas.

6. La información mencionada en el apartado 5 incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del producto con elementos digitales no conformes, el origen de ese producto con elementos digitales, la naturaleza de la supuesta no conformidad y del riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos formulados por el operador económico en cuestión. En particular, la autoridad de vigilancia del mercado indicará si la no conformidad se debe a uno o varios de los motivos siguientes:

   a) el incumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I por parte del producto con elementos digitales o de los procesos establecidos por el fabricante;

   b) deficiencias en las normas armonizadas, esquemas europeos de certificación de la ciberseguridad o especificaciones comunes a que se refiere el artículo 27.

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

8. Si, en el plazo de tres meses tras la recepción de la notificación indicada en el apartado 5 del presente artículo, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por un Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador económico correspondiente de conformidad con el artículo 18 del Reglamento (UE) 2019/1020.

9. Las autoridades de vigilancia del mercado de todos los Estados miembros se asegurarán de que las medidas restrictivas adecuadas respecto del producto con elementos digitales de que se trate, tales como la retirada de ese producto del mercado, se adopten sin demora.

Artículo 55

Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación a que hace referencia el artículo 54, apartado 5, un Estado miembro formule objeciones sobre una medida adoptada por otro Estado miembro, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora con el Estado miembro y el operador u operadores económicos pertinentes, y evaluará la medida nacional. Sobre la base de los resultados de la mencionada evaluación, la Comisión decidirá, en un plazo de nueve meses a partir de la notificación a que hace referencia el artículo 54, apartado 5, si la medida nacional está justificada o no, y notificará esa decisión al Estado miembro implicado.

2. Si la medida nacional se considera justificada, todos los Estados miembros adoptarán las medidas necesarias para garantizar la retirada de su mercado del producto con elementos digitales no conforme e informarán a la Comisión en consecuencia. Si la medida nacional se considera injustificada, el Estado miembro de que se trate retirará la medida.

3. Cuando la medida nacional se considere justificada y la no conformidad del producto con elementos digitales se atribuya a deficiencias de las normas armonizadas, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n.º 1025/2012.

4. Cuando la medida nacional se considere justificada y la no conformidad del producto con elementos digitales se atribuya a deficiencias de un esquema europeo de certificación de la ciberseguridad a que hace referencia el artículo 27, la Comisión estudiará la posibilidad de modificar o derogar el acto delegado adoptado en virtud del artículo 27, apartado 9, que especifique la presunción de conformidad en relación con dicho esquema de certificación.

5. Cuando la medida nacional se considere justificada y la no conformidad del producto con elementos digitales se atribuya a deficiencias de las especificaciones comunes a que hace referencia el artículo 27, la Comisión estudiará la posibilidad de modificar o derogar el acto de ejecución adoptado en virtud del artículo 27, apartado 2, por el que se establezcan dichas especificaciones comunes.

Artículo 56

Procedimiento a escala de la Unión aplicable a los productos con elementos digitales que presentan un riesgo de ciberseguridad significativo

1. Cuando la Comisión tenga un motivo suficiente para considerar, también sobre la base de la información facilitada por la ENISA, que un producto con elementos digitales que presenta un riesgo de ciberseguridad significativo no cumple los requisitos establecidos en el presente Reglamento, informará a las autoridades de vigilancia del mercado pertinentes. Cuando las autoridades de vigilancia del mercado lleven a cabo una evaluación de ese producto con elementos digitales que pueda presentar un riesgo de ciberseguridad significativo en lo que respecta a su conformidad con los requisitos establecidos en el presente Reglamento, se aplicarán los procedimientos a que se refieren los artículos 54 y 55.

2. Cuando la Comisión posea motivos suficientes para considerar que un producto con elementos digitales presenta un riesgo de ciberseguridad significativo a la luz de factores de riesgo no técnicos, informará a las autoridades de vigilancia del mercado competentes y, cuando proceda, a las autoridades competentes designadas o establecidas en virtud del artículo 8 de la Directiva (UE) 2022/2555 y cooperará con esas autoridades cuando sea necesario. La Comisión también considerará la pertinencia de los riesgos detectados para ese producto con elementos digitales en vista de sus tareas en relación con las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión previstas en el artículo 22 de la Directiva (UE) 2022/2555, y consultará, en caso necesario, al Grupo de Cooperación creado en virtud del artículo 14 de la Directiva (UE) 2022/2555 y a la ENISA.

3. En circunstancias que justifiquen una intervención inmediata para preservar el correcto funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto con elementos digitales a que hace referencia el apartado 1 sigue sin cumplir los requisitos establecidos en el presente Reglamento y que las autoridades de vigilancia del mercado pertinentes no han adoptado medidas eficaces, la Comisión llevará a cabo una evaluación del cumplimiento y podrá solicitar a la ENISA que facilite un análisis para apoyarla. La Comisión informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.

4. Sobre la base de la evaluación a que se refiere el apartado 3, la Comisión podrá establecer la necesidad de una medida correctora o restrictiva a escala de la Unión. A tal fin, consultará sin demora a los Estados miembros afectados y al operador u operadores económicos pertinentes.

5. Sobre la base de la consulta a que hace referencia el apartado 4 del presente artículo, la Comisión podrá adoptar actos de ejecución para prever medidas correctoras o restrictivas a escala de la Unión, como exigir la retirada del mercado de los productos con elementos digitales afectados o recuperarlos, en un plazo razonable, proporcional a la naturaleza del riesgo. Esos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

6. La Comisión comunicará inmediatamente los actos de ejecución a que hace referencia el apartado 5 al operador u operadores económicos pertinentes. Los Estados miembros aplicarán esos actos de ejecución sin demora e informarán de ello a la Comisión.

7. Los apartados 3 a 6 serán aplicables mientras dure la situación excepcional que haya justificado la intervención de la Comisión, siempre que el producto con elementos digitales en cuestión no se lleve a conformidad con lo dispuesto en el presente Reglamento.

Artículo 57

Productos con elementos digitales conformes
que presentan un riesgo de ciberseguridad significativo

1. La autoridad de vigilancia del mercado de un Estado miembro instará a un operador económico a que adopte todas las medidas adecuadas cuando, tras haber realizado una evaluación con arreglo al artículo 54, constate que, aunque un producto con elementos digitales y los procesos establecidos por el fabricante son conformes con el presente Reglamento, dicho producto presenta un riesgo de ciberseguridad significativo, y, además, plantean un riesgo para:

   a) la salud o la seguridad de las personas;

   b) el cumplimiento de las obligaciones que impone el Derecho nacional o de la Unión en materia de protección de los derechos fundamentales;

c) la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema electrónico de información por entidades esenciales a que se refiere el artículo 3, apartado 1, de la Directiva (UE) 2022/2555, u

d) otros aspectos relativos a la protección del interés público.

Las medidas a que se refiere el párrafo primero podrán incluir medidas para garantizar que el producto con elementos digitales en cuestión y los procesos establecidos por el fabricante ya no presenten los riesgos pertinentes cuando se comercialicen, o bien para retirarlos del mercado o recuperarlos en un plazo razonable, proporcional a la naturaleza del riesgo.

2. El fabricante u otros operadores económicos pertinentes se asegurarán de que se adoptan medidas correctoras con respecto a todos los productos con elementos digitales afectados que hayan comercializado en toda la Unión en el plazo establecido por la autoridad de vigilancia del mercado del Estado miembro a que hace referencia el apartado 1.

3. El Estado miembro informará inmediatamente a la Comisión y a los demás Estados miembros acerca de las medidas adoptadas de conformidad con el apartado 1. La información facilitada incluirá todos los detalles de que se disponga, en particular los datos necesarios para identificar los productos con elementos digitales en cuestión y para determinar su origen, su cadena de suministro, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión consultará sin demora a los Estados miembros y a los operadores económicos pertinentes y evaluará las medidas nacionales adoptadas. Sobre la base de los resultados de dicha evaluación, la Comisión decidirá si la medida está justificada o no y, en su caso, propondrá medidas adecuadas.

5. La Comisión dirigirá la decisión a que se refiere el apartado 4 a los Estados miembros.

6. Cuando la Comisión tenga un motivo suficiente para considerar, también sobre la base de la información facilitada por la ENISA, que un producto con elementos digitales, a pesar de ser conforme con el presente Reglamento, presenta los riesgos a que hace referencia el apartado 1 del presente artículo, informará a la autoridad o las autoridades de vigilancia del mercado pertinentes y podrá solicitarles que lleven a cabo una evaluación y sigan los procedimientos a que hacen referencia el artículo 54 y los apartados 1, 2 y 3 del presente artículo.

7. En circunstancias que justifiquen una intervención inmediata para preservar el correcto funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto con elementos digitales a que hace referencia el apartado 6 sigue presentando los riesgos a que hace referencia el apartado 1, y que las autoridades de vigilancia del mercado nacionales pertinentes no han adoptado medidas eficaces, la Comisión llevará a cabo una evaluación de los riesgos que presenta el producto con elementos digitales y podrá solicitar a la ENISA que proporcione una análisis para apoyar esa evaluación, e informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.

8. Sobre la base de la evaluación a que se refiere el apartado 7, la Comisión podrá establecer la necesidad de una medida correctora o restrictiva a escala de la Unión. A tal fin, consultará sin demora a los Estados miembros afectados y al operador u operadores económicos pertinentes.

9. Sobre la base de la consulta a que hace referencia el apartado 8 del presente artículo, la Comisión podrá adoptar actos de ejecución para decidir sobre medidas correctoras o restrictivas a escala de la Unión, como exigir la retirada del mercado o la recuperación de los productos con elementos digitales afectados en un plazo razonable, proporcional a la naturaleza del riesgo. Esos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

10. La Comisión comunicará inmediatamente los actos de ejecución a que hace referencia el apartado 9 al operador u operadores económicos pertinentes. Los Estados miembros aplicarán esos actos de ejecución sin demora e informarán de ello a la Comisión.

11. Los apartados 6 a 10 serán aplicables mientras dure la situación excepcional que haya justificado la intervención de la Comisión y mientras el producto con elementos digitales correspondiente siga presentando los riesgos a que hace referencia el apartado 1.

Artículo 58

Incumplimiento formal

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constate una de las situaciones indicadas a continuación, instará al fabricante correspondiente a que subsane el incumplimiento de que se trate:

a) la colocación del marcado CE no es conforme con los artículos 29 y 30;

b) no se ha colocado el marcado CE;

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

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

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

f) la documentación técnica no está disponible o está incompleta.

2. Cuando el incumplimiento indicado en el apartado 1 persista, el Estado miembro correspondiente adoptará todas las medidas adecuadas para restringir o prohibir la comercialización del producto con elementos digitales o asegurarse de que se recupera o se retira del mercado.

Artículo 59

Actividades conjuntas de las autoridades de vigilancia del mercado

1. Las autoridades de vigilancia del mercado podrán acordar con otras autoridades pertinentes la realización de actividades conjuntas con objeto de garantizar la ciberseguridad y la protección de los consumidores respecto de productos específicos con elementos digitales introducidos en el mercado o comercializados, en particular aquellos productos con elementos digitales que con frecuencia presentan riesgos de ciberseguridad.

2. La Comisión o la ENISA propondrán actividades conjuntas de control del cumplimiento del presente Reglamento que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre posibles incumplimientos en varios Estados miembros de los requisitos establecidos por el presente Reglamento por parte de los productos con elementos digitales que entran en el ámbito de aplicación de este.

3. Las autoridades de vigilancia del mercado y, en su caso, la Comisión se asegurarán de que el acuerdo para llevar a cabo las actividades conjuntas no conduzca a una competencia desleal entre los operadores económicos y no afecte negativamente a la objetividad, independencia e imparcialidad de las partes en el acuerdo.

4. Una autoridad de vigilancia del mercado podrá utilizar cualquier información obtenida como resultado de las actividades conjuntas llevadas a cabo como parte de cualquier investigación que realice.

5. La autoridad de vigilancia del mercado de que se trate y, en su caso, la Comisión publicarán el acuerdo sobre actividades conjuntas, incluidos los nombres de las partes.

Artículo 60

Barridos

1. Las autoridades de vigilancia del mercado llevarán a cabo acciones de control simultáneas coordinadas («barridos») de determinados productos con elementos digitales o categorías de estos para comprobar el cumplimiento o detectar infracciones del presente Reglamento. Estos barridos podrán incluir la inspección de productos con elementos digitales adquiridos bajo una identidad encubierta.

2. Salvo que las autoridades de vigilancia del mercado implicadas acuerden otra cosa, los barridos serán coordinados por la Comisión. El coordinador del barrido hará públicos, en su caso, los resultados agregados.

3. Cuando, en el desempeño de sus funciones, la ENISA determine, también sobre la base de las notificaciones recibidas en virtud del artículo 14, apartados 1 y 3, categorías de productos con elementos digitales para las que puedan organizarse barridos, presentará una propuesta de barrido al coordinador mencionado en el apartado 2 del presente artículo para su examen por las autoridades de vigilancia del mercado.

4. Cuando efectúen barridos, las autoridades de vigilancia del mercado participantes podrán ejercer las facultades de investigación contempladas en los artículos 52 a 58 y las demás facultades que les confiera el Derecho nacional.

5. Las autoridades de vigilancia del mercado podrán invitar a funcionarios de la Comisión y otros acompañantes autorizados por esta a participar en las operaciones de barrido.

Capítulo VI
Poderes delegados y procedimiento de comité

Artículo 61

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 los actos delegados mencionados en el artículo 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 y 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, y en el artículo 31, apartado 5, se otorgan a la Comisión por un período de cinco años a partir del … [*la fecha de entrada en vigor del presente Reglamento*]. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes a que hacen referencia el artículo 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 y 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, y el artículo 31, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de 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 en 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 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 o 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, o el artículo 31, apartado 5, entrarán en vigor únicamente si, en un plazo de dos 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 mencionado se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 62

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.

3. Cuando el dictamen del comité deba obtenerse mediante procedimiento escrito, se pondrá fin a dicho procedimiento sin resultado si, en el plazo para la emisión del dictamen, el presidente del comité así lo decide o si un miembro del comité así lo solicita.

Capítulo VII
Confidencialidad y sanciones

Artículo 63
Confidencialidad

1. Todas las partes involucradas en la aplicación del presente Reglamento 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 y la información empresarial confidencial o los secretos comerciales de las personas físicas o jurídicas, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo[36];

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

   c) los intereses públicos y de seguridad nacional;

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

[36] 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).

2. Sin perjuicio de lo dispuesto en el apartado 1, la información intercambiada de manera confidencial entre las autoridades de vigilancia del mercado y entre estas y la Comisión no se revelará sin el acuerdo previo de la autoridad de vigilancia del mercado de origen.

3. Los apartados 1 y 2 no afectarán a los derechos y obligaciones de la Comisión, los Estados miembros y los organismos notificados en lo que se refiere al intercambio de información y la difusión de advertencias, ni a las obligaciones de facilitar información que incumban a las personas interesadas en virtud del Derecho penal de los Estados miembros.

4. Cuando sea necesario, la Comisión y los Estados miembros podrán intercambiar información sensible con autoridades pertinentes de terceros países con las que hayan celebrado acuerdos de confidencialidad bilaterales o multilaterales que garanticen un nivel de protección adecuado.

Artículo 64

Sanciones

1. Los Estados miembros establecerán el régimen de sanciones aplicables a las infracciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Tales sanciones serán efectivas, proporcionadas y disuasorias. Los Estados miembros comunicarán sin demora a la Comisión el régimen establecido y las medidas adoptadas, y le notificarán sin demora toda modificación posterior.

2. El incumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I y de las obligaciones establecidas en los artículos 13 y 14 estará sujeto a multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 2,5 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior.

3. El incumplimiento de las obligaciones establecidas en los artículos 18 a 23, el artículo 28, el artículo 30, apartados 1 a 4, el artículo 31, apartados 1 a 4, el artículo 32, apartados 1, 2 y 3, el artículo 33, apartado 5, y los artículos 39, 41, 47, 49 y 53 será objeto a multas administrativas de hasta 10 000 000 EUR o, si el infractor es una empresa, de hasta el 2 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior.

4. La presentación de información incorrecta, incompleta o engañosa a organismos notificados y a las autoridades de vigilancia del mercado en respuesta a una solicitud será objeto de multas administrativas de hasta 5 000 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior.

5. Al decidir la cuantía de la multa administrativa en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación correspondiente y se tendrá debidamente en cuenta lo siguiente:

   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

   b) si las mismas u otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador económico por una infracción similar;

   c) el tamaño, en particular por lo que respecta a las microempresas y las pequeñas y medianas empresas, incluidas las empresas emergentes, y la cuota de mercado del operador económico que comete la infracción.

6. Las autoridades de vigilancia del mercado que apliquen multas administrativas informarán de esta aplicación a las autoridades de vigilancia del mercado de otros Estados miembros por medio del sistema de información y comunicación a que hace referencia el artículo 34 del Reglamento (UE) 2019/1020.

7. Cada Estado miembro establecerá normas que determinen si es posible, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que las multas las impongan órganos jurisdiccionales nacionales competentes u otros organismos, según las competencias establecidas a nivel nacional en dichos Estados miembros. La aplicación de dichas normas en estos Estados miembros tendrá un efecto equivalente.

9. Según las circunstancias de cada caso concreto, podrán imponerse multas administrativas de manera adicional a cualquier otra medida correctora o restrictiva aplicada por las autoridades de vigilancia del mercado por la misma infracción.

10. Como excepción a lo dispuesto en los apartados 3 a 9, las multas administrativas a que se refieren esos apartados no se aplicarán a:

    a) los fabricantes que se consideren microempresas o pequeñas empresas en relación con cualquier incumplimiento de los plazos a que se refieren el artículo 14, apartado 2, letra a), o el artículo 14, apartado 4, letra a);

    b) cualquier infracción del presente Reglamento por parte de administradores de comunidad de programas informáticos de código abierto.

Artículo 65

Acciones de representación

La Directiva (UE) 2020/1828 se aplicará a las acciones de representación ejercitadas frente a infracciones por parte de operadores económicos de las disposiciones del presente Reglamento que perjudiquen o puedan perjudicar los intereses colectivos de los consumidores.

Capítulo VIII

Disposiciones transitorias y finales

Artículo 66

Modificación del Reglamento (UE) 2019/1020

En el anexo I del Reglamento (UE) 2019/1020, se añade el punto siguiente:

«XX[+]. Reglamento (UE) 2024/… del Parlamento Europeo y del Consejo[*++].

---

[*] Reglamento (UE) 2024/… del Parlamento Europeo y del Consejo, de …, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, …, ELI: …).».

[+] DO: insértese en el texto el número consecutivo al último de la lista del anexo I del Reglamento (UE) 2019/1020.

[++] DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 100/23 [2022/0272(COD)] e insértense en la nota a pie de página el número de orden, la fecha y la referencia de publicación en el DO de dicho Reglamento.

Artículo 67

Modificación de la Directiva (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 se añade el punto siguiente:

«XX[+]. Reglamento (UE) 2024/… del Parlamento Europeo y del Consejo[*++].

---

[*] Reglamento (UE) 2024/… del Parlamento Europeo y del Consejo, de …, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, …, ELI: …).».

[+] DO: insértese en el texto el número consecutivo al último de la lista del anexo I de la Directiva (UE) 2020/1828.

[++] DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 100/23 [2022/0272(COD)] e insértense en la nota a pie de página el número de orden, la fecha y la referencia de publicación en el DO de dicho Reglamento.

Artículo 68

Modificación del Reglamento (UE) n.º 168/2013

El anexo II del Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo[37] se modifica como sigue:

En el cuadro de la parte C1, se añade la entrada siguiente:

«

XX+	18	Protección del vehículo frente a ciberataques		x	x	x	x	x	x	x	x	x	x	x	x	x	x

».

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

+ DO: insértese en el texto el número consecutivo al último de la parte C1 del anexo II del Reglamento (UE) n.º 168/2013.

Artículo 69

Disposiciones transitorias

1. Los certificados de examen de tipo UE y las decisiones de aprobación expedidos en relación con los requisitos de ciberseguridad para productos con elementos digitales que estén sujetos a otra legislación de armonización de la Unión distintas del presente Reglamento seguirán siendo válidos hasta el … [*cuarenta y dos meses desde la fecha de entrada en vigor del presente Reglamento*], salvo que caduquen con anterioridad a esa fecha o salvo que se indique lo contrario en esa legislación de armonización de la Unión, en cuyo caso seguirán siendo válidos según lo que disponga dicha legislación de la Unión.

2. Los productos con elementos digitales que hayan sido introducidos en el mercado antes del … [*treinta y seis meses desde la fecha de entrada en vigor del presente Reglamento*] estarán sujetos a los requisitos establecidos en el presente Reglamento únicamente si, a partir de dicha fecha, los productos mencionados se ven sometidos a una modificación sustancial.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, las obligaciones establecidas en el artículo 14 se aplicarán a todos los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento y hayan sido introducidos en el mercado antes del … [*treinta y seis meses desde la entrada en vigor del presente Reglamento*].

Artículo 70

Evaluación y revisión

1. A más tardar el … [*setenta y dos meses desde la fecha de aplicación del presente Reglamento*], y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

2. A más tardar el … [*cuarenta y cinco meses desde la fecha de entrada en vigor del presente Reglamento*], la Comisión, previa consulta a la ENISA y a la red de CSIRT, presentará un informe al Parlamento Europeo y al Consejo en el que se evalúe la eficacia de la plataforma única de notificación establecida en el artículo 16, así como las repercusiones de la aplicación de los motivos relacionados con la ciberseguridad a que se refiere el artículo 16, apartado 2, por parte de los CSIRT designados como coordinadores en la eficacia de la plataforma única de notificación en lo que respecta a la difusión oportuna de las notificaciones recibidas a otros CSIRT pertinentes.

Artículo 71

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento será aplicable a partir del … [*treinta y seis meses desde la fecha de entrada en vigor del presente Reglamento*].

   No obstante, el artículo 14 será aplicable a partir del … [*veintiún meses desde la fecha de entrada en vigor del presente Reglamento*] y el capítulo IV (artículo 35 a 51) será aplicable a partir del … [*dieciocho meses desde la entrada en vigor del presente Reglamento*].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en …, el

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*El Presidente*

ANEXO I

REQUISITOS ESENCIALES DE CIBERSEGURIDAD

Parte I Requisitos de ciberseguridad relativos a las propiedades de los productos con elementos digitales

1) Los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes.

2) Sobre la base de la evaluación de riesgos de ciberseguridad a la que hace referencia el artículo 13, apartado 2, y cuando proceda, los productos con elementos digitales:

   a) se comercializarán sin vulnerabilidades aprovechables conocidas;

   b) se comercializarán con una configuración segura por defecto, a menos que el fabricante y el usuario profesional acuerden otra cosa en relación con un producto a medida con elementos digitales, incluida la posibilidad de restablecer el producto a su estado original;

   c) garantizarán que las vulnerabilidades puedan abordarse mediante actualizaciones de seguridad, incluidas, cuando proceda, las actualizaciones automáticas de seguridad instaladas en un plazo adecuado habilitadas como configuración por defecto, con un mecanismo de exclusión voluntaria claro y fácil de utilizar, mediante la notificación de las actualizaciones disponibles a los usuarios y la opción de posponerlas temporalmente;

d) garantizarán la protección contra el acceso no autorizado mediante mecanismos de control adecuados, incluidos, entre otros, sistemas de gestión de la autenticación, la identidad o el acceso, e informarán de posibles accesos no autorizados;

e) protegerán la confidencialidad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, mediante, por ejemplo, el cifrado de los datos en reposo o en tránsito pertinentes por medio de mecanismos de última tecnología, o mediante la utilización de otros medios técnicos;

f) protegerán la integridad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, los comandos, los programas y la configuración frente a toda manipulación o modificación no autorizada por el usuario, e informarán sobre los casos de corrupción de datos;

g) tratarán únicamente los datos personales o de otro tipo que sean adecuados, pertinentes y limitados a lo que sea necesario para la finalidad prevista del producto con elementos digitales («minimización de datos»);

h) protegerán la disponibilidad de funciones esenciales y básicas, también tras un incidente, también mediante medidas de resiliencia frente a ataques de denegación de servicio y paliativas de sus efectos;

i) minimizarán las repercusiones negativas de los propios productos o de los dispositivos conectados en la disponibilidad de servicios prestados por otros dispositivos o redes;

j) estarán diseñados, desarrollados y producidos para limitar las superficies de ataque, incluidas las interfaces externas;

k) estarán diseñados, desarrollados y producidos para reducir el impacto de un incidente, por medio de mecanismos y técnicas adecuados para paliar el aprovechamiento de las vulnerabilidades;

l) proporcionarán información relacionada con la seguridad mediante el registro o el seguimiento de la actividad interna pertinente, incluidos el acceso a datos, servicios o funciones y la modificación de estos, con un mecanismo de exclusión voluntaria para el usuario;

m) ofrecerán a los usuarios la posibilidad de eliminar de manera segura y fácil, de forma permanente, todos los datos y parámetros y, cuando esos datos puedan transferirse a otros productos o sistemas, garantizarán que esto se haga de manera segura.

Parte II Requisitos de gestión de las vulnerabilidades

Los fabricantes de los productos con elementos digitales:

1) identificarán y documentarán las vulnerabilidades y los componentes presentes en el producto con elementos digitales, también mediante la elaboración de una nomenclatura de materiales de los programas informáticos en un formato comúnmente utilizado y legible por máquina, que incluya, como mínimo, las dependencias de máximo nivel del producto;

2) por lo que respecta a los riesgos para los productos con elementos digitales, abordarán y subsanarán las vulnerabilidades sin demora, también mediante la provisión de actualizaciones de seguridad; cuando sea técnicamente viable, las nuevas actualizaciones de seguridad se facilitarán por separado con respecto a las actualizaciones de funcionalidad;

3) llevarán a cabo exámenes y pruebas eficaces y periódicos de la seguridad del producto con elementos digitales;

4) una vez esté disponible una actualización de seguridad, compartirán y divulgarán públicamente información sobre las vulnerabilidades solucionadas, incluidas una descripción de las vulnerabilidades, información que permita a los usuarios identificar el producto con elementos digitales afectado, las repercusiones y la gravedad de las vulnerabilidades e información clara y accesible que ayude a los usuarios a corregir las vulnerabilidades; en casos debidamente justificados, cuando los fabricantes consideren que los riesgos para la seguridad de la publicación superan los beneficios en materia de seguridad, podrán retrasar la publicación de información sobre una vulnerabilidad solucionada hasta que se haya dado a los usuarios la posibilidad de aplicar el parche correspondiente;

5) pondrán en marcha y aplicarán una política de divulgación coordinada de vulnerabilidades;

6) adoptarán medidas para facilitar el intercambio de información sobre posibles vulnerabilidades de su producto con elementos digitales, así como de los componentes de terceros presentes en el producto, también proporcionando una dirección de contacto para la notificación de las vulnerabilidades descubiertas en el producto con elementos digitales;

7) preverán mecanismos para distribuir de manera segura las actualizaciones de los productos con elementos digitales, con el fin de garantizar que las vulnerabilidades se solucionen o se reduzcan de manera oportuna y, cuando proceda para las actualizaciones automáticas, de una manera automática;

8) garantizarán que, cuando se disponga de actualizaciones de seguridad para hacer frente a los problemas de seguridad detectados, estos se difundan sin demora y, a menos que el fabricante y el usuario profesional acuerden otra cosa en relación con un producto a medida con elementos digitales, de forma gratuita, acompañados de mensajes de aviso que proporcionen a los usuarios la información pertinente, también en relación con las posibles medidas que deban adoptarse.

ANEXO II

INFORMACIÓN E INSTRUCCIONES PARA EL USUARIO

Junto al producto con elementos digitales, se especificará, como mínimo:

1. el nombre, nombre comercial registrado o marca registrada del fabricante, la dirección postal, la dirección de correo electrónico u otro contacto digital, así como, cuando esté disponible, el sitio web en el que se puede contactar con el fabricante;

2. el punto único de contacto en el que pueda notificarse y obtenerse información sobre las vulnerabilidades del producto con elementos digitales, y el lugar en que puede encontrarse la política del fabricante respecto a las vulnerabilidades coordinadas;

3. el nombre y el tipo del producto con elementos digitales, y toda información adicional que permita su identificación única;

4. la finalidad prevista del producto con elementos digitales, incluido el entorno de seguridad proporcionado por el fabricante, así como las funcionalidades esenciales del producto e información sobre sus propiedades de seguridad;

5. cualquier circunstancia conocida o previsible, asociada al uso del producto con elementos digitales conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos de ciberseguridad significativos;

6. cuando proceda, la dirección de internet en la que puede accederse a la declaración UE de conformidad;

7. el tipo de apoyo técnico en materia de seguridad ofrecido por el fabricante y la fecha de finalización del período de soporte durante el que está previsto que se gestionen las vulnerabilidades y que los usuarios puedan recibir actualizaciones de seguridad;

8. instrucciones detalladas o una dirección de internet en la que se especifiquen dichas instrucciones e información sobre:

   a) las medidas necesarias durante la puesta en servicio inicial y a lo largo de toda la vida del producto con elementos digitales para garantizar su uso seguro;

   b) cómo los cambios en el producto con elementos digitales pueden afectar a la seguridad de los datos;

   c) cómo pueden instalarse las actualizaciones pertinentes para la seguridad;

   d) cómo realizar la retirada del servicio del producto con elementos digitales de forma segura, incluida información sobre cómo pueden eliminarse de forma segura los datos de los usuarios;

   e) cómo puede apagarse la configuración por defecto que permite la instalación automática de actualizaciones de seguridad, tal como se exige en el anexo I, parte I, punto 2, letra c);

   f) cuando el producto con elementos digitales esté destinado a integrarse en otros productos con elementos digitales, la información necesaria para que el integrador cumpla los requisitos esenciales de ciberseguridad establecidos en el anexo I y los requisitos de documentación establecidos en el anexo VII;

9. si el fabricante decide poner a disposición del usuario la nomenclatura de materiales de los programas informáticos, información sobre dónde puede consultarse esta.

ANEXO III

PRODUCTOS IMPORTANTES CON ELEMENTOS DIGITALES

Clase I

1. Sistemas de gestión de la identidad y programas y equipos informáticos de gestión de accesos privilegiados, incluidos los lectores de autenticación y control de acceso, como los lectores biométricos

2. Navegadores independientes e integrados

3. Gestores de contraseñas

4. Programas informáticos que busquen, eliminen o pongan en cuarentena programas maliciosos

5. Productos con elementos digitales que ejerzan la función de red privada virtual (VPN, por sus siglas en inglés)

6. Sistemas de gestión de redes

7. Sistemas de gestión de información de seguridad y eventos (SIEM, por sus siglas en inglés)

8. Gestores de arranque

9. Infraestructuras públicas clave y programas informáticos de emisión de certificados digitales

10. Interfaces físicas y virtuales de red

11. Sistemas operativos

12. Enrutadores, módems destinados a la conexión a internet e interruptores

13. Microprocesadores con funcionalidades relacionadas con la seguridad

14. Microcontroladores con funcionalidades relacionadas con la seguridad

15. Circuitos integrados de aplicación específica (ASIC, por sus siglas en inglés) y matrices de puertas programables *in situ* (FPGA, por sus siglas en inglés) con funcionalidades relacionadas con la seguridad

16. Asistentes virtuales de propósito general para hogares inteligentes

17. Productos para hogares inteligentes con funciones de seguridad, como cerraduras, cámaras de seguridad, sistemas de vigilancia de bebés y sistemas de alarma inteligentes

18. Juguetes conectados a internet regulados por la Directiva 2009/48/CE del Parlamento Europeo y del Consejo[1] que tienen funcionalidades sociales interactivas (por ejemplo, que hablen o filmen) o que funcionalidades de seguimiento de localización

19. Productos ponibles personales destinados a ser utilizados o colocados en el cuerpo humano con fines de seguimiento médico (como la localización) y a los que no se aplican el Reglamento (UE) 2017/745 o el Reglamento (UE) 2017/746, o productos ponibles personales destinados a ser utilizados por y para niños.

Clase II

1. Hipervisores y sistemas de ejecución de contenedores que permitan la ejecución virtualizada de sistemas operativos y entornos similares

2. Cortafuegos y sistemas de detección y prevención de intrusiones

3. Microprocesadores resistentes a las manipulaciones

4. Microcontroladores resistentes a las manipulaciones.

---

[1] Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes (DO L 170 de 30.6.2009, p. 1).

ANEXO IV

PRODUCTOS CRÍTICOS CON ELEMENTOS DIGITALES

1. Dispositivos de equipos informáticos con cajas de seguridad

2. Pasarelas de contadores inteligentes dentro de los sistemas de medición inteligente según se definen en el artículo 2, punto 23, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo[1], y otros dispositivos con fines de seguridad avanzada, incluido el procesamiento seguro de criptoactivos

3. Tarjetas inteligentes o dispositivos similares, que incluyan elementos seguros.

---

[1] Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE (DO L 158 de 14.6.2019, p. 125).

ANEXO V

DECLARACIÓN UE DE CONFORMIDAD

La declaración UE de conformidad a que hace referencia el artículo 28 contendrá toda la información siguiente:

1. El nombre y el tipo del producto con elementos digitales, y toda información adicional que permita su identificación única.

2. Nombre y dirección del fabricante o de su representante autorizado.

3. La afirmación de que la declaración UE de conformidad se emite bajo la exclusiva responsabilidad del proveedor.

4. El objeto de la declaración (identificación del producto con elementos digitales que permita la trazabilidad, lo que podrá incluir, cuando proceda, una fotografía).

5. La afirmación de que el objeto de la declaración descrito anteriormente es conforme a la legislación de armonización de la Unión pertinentes.

6. Referencias a todas las normas armonizadas pertinentes utilizadas o a cualquier otra especificación común o certificación de la ciberseguridad respecto a las cuales se declara la conformidad.

7. En su caso, el nombre y número del organismo notificado, una descripción del procedimiento de evaluación de la conformidad llevado a cabo y la identificación del certificado emitido.

8. Información adicional:

Firmado por y en nombre de: ……

(lugar y fecha de expedición):

(nombre, cargo) (firma):

ANEXO VI

DECLARACIÓN UE DE CONFORMIDAD SIMPLIFICADA

La declaración UE de conformidad simplificada contemplada en el artículo 13, apartado 20, se ajustará a lo siguiente:

Por la presente, [nombre del fabricante] declara que el tipo de producto con elementos digitales [designación del tipo de producto con elemento digital] es conforme con el Reglamento (UE) …/… del Parlamento Europeo y del Consejo[1].

El texto completo de la declaración UE de conformidad está disponible en la dirección Internet siguiente:

---

[1] DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 100/23 [2022/0272(COD)].

ANEXO VII

CONTENIDO DE LA DOCUMENTACIÓN TÉCNICA

La documentación técnica a que hace referencia el artículo 31 contendrá como mínimo la siguiente información, en función del producto con elementos digitales de que se trate:

1. una descripción general del producto con elementos digitales, incluidas:

   a) su finalidad prevista;

   b) las versiones de los programas informáticos que afecten al cumplimiento de los requisitos esenciales de ciberseguridad;

   c) cuando el producto con elementos digitales sea un producto consistente en equipos informáticos, fotografías o ilustraciones que muestren las características externas, el marcado y la configuración interna;

   d) la información y las instrucciones para el usuario indicadas en el anexo II;

2. una descripción del diseño, el desarrollo y la producción del producto con elementos digitales y de los procesos de gestión de las vulnerabilidades, que incluya:

   a) información necesaria sobre el diseño y el desarrollo del producto con elementos digitales, incluidos, en su caso, planos y esquemas, y una descripción de la arquitectura del sistema que explique cómo se apoyan o se alimentan mutuamente los componentes de los programas informáticos y cómo se integran en el tratamiento general;

b) información y especificaciones necesarias de los procesos de gestión de las vulnerabilidades establecidos por el fabricante, incluida la nomenclatura de materiales de los programas informáticos, la política de divulgación coordinada de vulnerabilidades, pruebas de que se ha facilitado una dirección de contacto para la notificación de vulnerabilidades y una descripción de las soluciones técnicas elegidas para la distribución segura de las actualizaciones;

c) información y especificaciones necesarias de los procesos de producción y seguimiento del producto con elementos digitales y la validación de esos procesos;

3. una evaluación de los riesgos de ciberseguridad frente a los cuales se haya diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, en virtud del artículo 13, también en lo que ataña al modo en que son aplicables los requisitos esenciales de ciberseguridad formulados en el anexo I, parte I;

4. información pertinente que se haya tenido en cuenta para determinar el período de soporte en virtud del artículo 13, apartado 8, del producto con elementos digitales;

5. una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, las especificaciones comunes tal como se definen en el artículo 27 del presente Reglamento o los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 de conformidad con el artículo 27, apartado 8, del presente Reglamento y, cuando no se hayan aplicado esas normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad, la descripción de las soluciones adoptadas para cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I, partes I y II, junto con una lista de otras especificaciones técnicas pertinentes aplicadas; en caso de normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad que se apliquen parcialmente, se especificarán en la documentación técnica las partes que se hayan aplicado;

6. informes de las pruebas realizadas para verificar la conformidad del producto con elementos digitales y de los procesos de gestión de las vulnerabilidades con los requisitos esenciales de ciberseguridad aplicables que se establecen en el anexo I, partes I y II;

7. una copia de la declaración UE de conformidad;

8. cuando proceda, la nomenclatura de materiales de los programas informáticos, previa solicitud motivada por parte de una autoridad de vigilancia del mercado, siempre que sea necesario para que dicha autoridad pueda comprobar el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I.

ANEXO VIII

PROCEDIMIENTOS DE EVALUACIÓN DE LA CONFORMIDAD

Parte I Procedimiento de evaluación de la conformidad basado en el control interno (basado en el módulo A)

1. El control interno es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2, 3 y 4 de la presente parte, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos con elementos digitales son conformes con todos los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y que el fabricante cumple los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

2. El fabricante elaborará la documentación técnica descrita en el anexo VII.

3. Diseño, desarrollo, producción de los productos con elementos digitales y gestión de las vulnerabilidades

   El fabricante adoptará todas las medidas necesarias para que los procesos de diseño, desarrollo, producción y gestión de las vulnerabilidades, así como el seguimiento de dichos procesos, garanticen la conformidad de los productos con elementos digitales fabricados o desarrollados y de los procesos establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, partes I y II.

4. Marcado de conformidad y declaración de conformidad

4.1. El fabricante colocará el marcado CE en cada producto con elementos digitales que satisfaga los requisitos aplicables establecidos en el presente Reglamento.

4.2. El fabricante redactará una declaración UE de conformidad por escrito para cada producto con elementos digitales de conformidad con el artículo 28 y la mantendrá, junto con la documentación técnica, a disposición de las autoridades nacionales durante un período de diez años después de la introducción en el mercado del producto con elementos digitales o el período de soporte, si este fuese más prolongado. En la declaración UE de conformidad se identificará el producto con elementos digitales para el cual haya sido elaborada. Se facilitará una copia de la declaración CE de conformidad a las autoridades competentes que lo soliciten.

5. Representantes autorizados

Las obligaciones del fabricante establecidas en el punto 4 podrá cumplirlas, en su nombre y bajo su responsabilidad, su representante autorizado, siempre que las obligaciones pertinentes estén especificadas en el mandato.

Parte II Examen de tipo UE (basado en el módulo B)

1. El examen de tipo UE es la parte de un procedimiento de evaluación de la conformidad mediante la cual un organismo notificado examina el diseño técnico y el desarrollo de un producto con elementos digitales y los procesos de gestión de las vulnerabilidades establecidos por el fabricante, y certifica que un producto con elementos digitales cumple los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y que el fabricante cumple los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

2. El examen de tipo UE se llevará a cabo mediante una evaluación de la adecuación del diseño técnico y el desarrollo del producto con elementos digitales a través del examen de la documentación técnica y las pruebas de apoyo a que se refiere el punto 3, más el examen de las muestras de una o varias partes críticas del producto (combinación del tipo de producción y el tipo de diseño).

3. El fabricante deberá presentar una solicitud de examen de tipo UE a un organismo notificado único de su elección.

   La solicitud incluirá:

   3.1. El nombre y la dirección del fabricante y, si la solicitud la presenta el representante autorizado, también el nombre y la dirección de este.

3.2. Una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.3. La documentación técnica, que permitirá evaluar la conformidad del producto con elementos digitales con los requisitos esenciales de ciberseguridad aplicables establecidos en el anexo I, parte I, y los procesos de gestión de las vulnerabilidades por parte del fabricante establecidos en el anexo I, parte II, e incluirá un análisis y una evaluación adecuados del riesgo o riesgos. Especificará los requisitos aplicables y contemplará, en la medida en que sea pertinente para la evaluación, el diseño, la fabricación y el funcionamiento del producto con elementos digitales. Incluirá, cuando proceda, al menos los elementos establecidos en el anexo VII.

3.4. Pruebas que acrediten la adecuación de las soluciones técnicas de diseño y desarrollo y de los procesos de gestión de las vulnerabilidades. Estas pruebas mencionarán todos los documentos que se hayan utilizado, en particular, en caso de que las normas armonizadas pertinentes o las especificaciones técnicas no se hayan aplicado íntegramente. Las pruebas incluirán, en caso necesario, los resultados de las pruebas realizadas por el laboratorio apropiado del fabricante o por otro laboratorio de pruebas en su nombre y bajo su responsabilidad.

4. El organismo notificado:

4.1. examinará la documentación técnica y las pruebas para evaluar la adecuación del diseño técnico y del desarrollo del producto con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y la adecuación de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II;

4.2. comprobará que las muestras se han desarrollado o fabricado conforme a la documentación técnica, e identificará los elementos que se han diseñado y desarrollado con arreglo a las disposiciones aplicables de las normas armonizadas o especificaciones técnicas pertinentes, así como los elementos que se han diseñado y desarrollado sin aplicar las disposiciones pertinentes de dichas normas;

4.3. efectuará, o hará que se efectúen, los exámenes y pruebas oportunos para comprobar si, cuando el fabricante haya optado por aplicar las soluciones de las normas armonizadas o especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, su aplicación ha sido correcta;

4.4. efectuará, o hará que se efectúen, los exámenes y pruebas oportunas para comprobar si, en caso de que no se hayan aplicado las soluciones de las normas armonizadas o especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, las soluciones adoptadas por el fabricante cumplen los requisitos esenciales de ciberseguridad correspondientes;

4.5. acordará con el fabricante el lugar donde se realizarán los exámenes y las pruebas.

5. El organismo notificado elaborará un informe de evaluación que recoja las actividades realizadas de conformidad con el punto 4 y sus resultados. Sin perjuicio de sus obligaciones frente a las autoridades notificantes, el organismo notificado solo dará a conocer el contenido del informe, íntegramente o en parte, con el acuerdo del fabricante.

6. Si el tipo y los procesos de gestión de las vulnerabilidades cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, el organismo notificado expedirá al fabricante un certificado de examen de tipo UE. El certificado incluirá el nombre y la dirección del fabricante, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para la identificación del tipo aprobado y de los procesos de gestión de las vulnerabilidades. Se podrán adjuntar al certificado uno o varios anexos.

El certificado y sus anexos contendrán toda la información pertinente que permita evaluar la conformidad de los productos con elementos digitales fabricados o desarrollados con el tipo examinado y los procesos de gestión de las vulnerabilidades, y permitir el control en servicio.

En caso de que el tipo y los procesos de gestión de las vulnerabilidades no cumplan los requisitos esenciales de ciberseguridad aplicables establecidos en el anexo I, el organismo notificado se negará a expedir un certificado de examen de tipo UE e informará de ello al solicitante, explicando detalladamente su negativa.

7. El organismo notificado se mantendrá informado de las actualizaciones de la última tecnología conocida que indiquen que el tipo aprobado y los procesos de gestión de las vulnerabilidades ya no pueden cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I del presente Reglamento, y determinará si tales cambios requieren más investigaciones. En ese caso, el organismo notificado informará al fabricante en consecuencia.

El fabricante informará al organismo notificado en posesión de la documentación técnica relativa al certificado de examen de tipo UE de todas las modificaciones del tipo aprobado y los procesos de gestión de las vulnerabilidades que puedan afectar a la conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I o las condiciones de validez del certificado. Tales modificaciones requerirán una aprobación adicional en forma de suplemento al certificado original de examen de tipo UE.

8. El organismo notificado llevará a cabo auditorías periódicas para garantizar que los procesos de gestión de las vulnerabilidades establecidos en el anexo I, parte II, se aplican adecuadamente.

9. Cada organismo notificado informará a sus autoridades notificantes sobre los certificados de examen de tipo UE o cualquier añadido o añadidos a ellos que haya expedido o retirado, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de certificados o añadidos que hayan sido rechazados, suspendidos o restringidos de otro modo.

Cada organismo notificado informará a los demás organismos notificados sobre los certificados de examen de tipo UE o los añadidos a estos certificados que haya rechazado, retirado, suspendido o restringido de otro modo, y, previa solicitud, sobre los certificados o sus añadidos que haya expedido.

La Comisión, los Estados miembros y los demás organismos notificados podrán, previa solicitud, obtener una copia de los certificados de examen de tipo UE o cualquiera de sus suplementos. Previa solicitud, la Comisión y los Estados miembros podrán obtener una copia de la documentación técnica y los resultados de los exámenes efectuados por el organismo notificado. El organismo notificado conservará una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como del expediente técnico que incluya la documentación presentada por el fabricante hasta el final de la validez del certificado.

10. El fabricante conservará a disposición de las autoridades nacionales una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como la documentación técnica durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado.

11. El representante autorizado del fabricante podrá presentar la solicitud a que se refiere el punto 3 y cumplir las obligaciones contempladas en los puntos 7 y 10, siempre que las obligaciones pertinentes estén especificadas en su mandato.

Parte III Conformidad con el tipo basada en el control interno de la producción (basada en el módulo C)

1. La conformidad con el tipo basada en el control interno de la producción es la parte del procedimiento de evaluación de la conformidad según la cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 3 de la presente parte, y garantiza y declara que los productos con elementos digitales en cuestión son conformes con el tipo descrito en el certificado de examen de tipo UE y cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y que los fabricantes cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

2. Producción

El fabricante tomará todas las medidas necesarias para que la producción y su seguimiento garanticen la conformidad de los productos con elementos digitales fabricados con el tipo aprobado descrito en el certificado de examen de tipo UE y con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y garantizará que los fabricantes cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

3. Marcado de conformidad y declaración de conformidad

3.1. El fabricante colocará el marcado CE en los productos con elementos digitales que sean conformes al tipo descrito en el certificado de examen de tipo UE y satisfagan los requisitos aplicables establecidos en el instrumento legislativo.

3.2. El fabricante redactará una declaración de conformidad para un modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada. Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

4. Representante autorizado

Las obligaciones del fabricante establecidas en el punto 3 podrá cumplirlas su representante autorizado, en su nombre y bajo su responsabilidad, siempre que las obligaciones pertinentes estén especificadas en su mandato.

Parte IV Conformidad basada en el aseguramiento de calidad total (basada en el módulo H)

1. La conformidad basada en el aseguramiento de calidad total es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 5 de la presente parte, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos con elementos digitales (o las categorías de productos) en cuestión son conformes con los requisitos establecidos en el anexo I, parte I, y que los procesos de gestión de las vulnerabilidades establecidos por el fabricante cumplen los requisitos establecidos en el anexo I, parte II.

2. Diseño, desarrollo, producción de los productos con elementos digitales y gestión de las vulnerabilidades

El fabricante aplicará un sistema de calidad aprobado, tal como se especifica en el punto 3, para el diseño, el desarrollo, la producción y la inspección y prueba finales de los productos con elementos digitales en cuestión y la gestión de las vulnerabilidades, lo mantendrá operativo a lo largo de todo el período de soporte y estará sujeto a la supervisión especificada en el punto 4.

3. Sistema de calidad

3.1. El fabricante presentará una solicitud de evaluación de su sistema de calidad ante el organismo notificado de su elección, para los productos con elementos digitales de que se trate.

La solicitud incluirá:

– el nombre y la dirección del fabricante y, si la solicitud la presenta el representante autorizado, también el nombre y la dirección de este,

– la documentación técnica para un modelo de cada categoría de productos con elementos digitales que se pretenda fabricar o desarrollar. La documentación técnica incluirá, cuando proceda, al menos los elementos establecidos en el anexo VII,

– la documentación relativa al sistema de calidad, y

– una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de calidad garantizará la conformidad de los productos con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y la conformidad de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos establecidos en el anexo I, parte II.

Todos los elementos, requisitos y disposiciones adoptados por el fabricante deberán reunirse de forma sistemática y ordenada en una documentación compuesta por políticas, procedimientos e instrucciones por escrito. Esta documentación del sistema de calidad permitirá una interpretación coherente de los programas, planes, manuales y registros de calidad.

En particular, incluirá una descripción adecuada de:

– los objetivos de calidad, el organigrama y las responsabilidades y competencias del personal de gestión en lo que se refiere al diseño, el desarrollo, la calidad del producto y la gestión de las vulnerabilidades,

– las especificaciones técnicas de diseño y desarrollo, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios que se utilizarán para asegurarse de que se cumplan los requisitos esenciales de ciberseguridad del anexo I, parte I, aplicables a los productos con elementos digitales,

– las especificaciones de procedimiento, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios que se utilizarán para asegurarse de que se cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II, aplicables al fabricante,

– las técnicas de control y verificación del diseño y el desarrollo, los procesos y las medidas sistemáticas que se vayan a utilizar en el diseño y el desarrollo de los productos con elementos digitales por lo que se refiere a la categoría de productos de que se trate,

– las correspondientes técnicas, procesos y actividades sistemáticas de producción, control de la calidad y aseguramiento de la calidad que se utilizarán,

– los exámenes y las pruebas que se efectuarán antes, durante y después de la producción, y su frecuencia,

– los expedientes de calidad, como los informes de inspección y datos de pruebas, los datos de calibrado y los informes sobre la cualificación del personal implicado,

– los medios con los que se hace el seguimiento de la consecución del diseño y de la calidad exigidos de los productos y del funcionamiento eficaz del sistema de calidad.

3.3. El organismo notificado evaluará el sistema de calidad para determinar si cumple los requisitos a que se refiere el punto 3.2.

Dará por supuesta la conformidad con dichos requisitos de los elementos del sistema de calidad que cumplan las especificaciones correspondientes de la norma nacional que transponga la norma armonizada o la especificación técnica pertinente.

Además de experiencia en sistemas de gestión de la calidad, el equipo de auditoría tendrá, como mínimo, un miembro con experiencia como evaluador en el campo del producto pertinente y la tecnología del producto en cuestión, así como tendrá el conocimiento de los requisitos aplicables establecidos en el presente Reglamento. La auditoría incluirá una visita de evaluación a las instalaciones del fabricante, siempre que estas existan. El equipo de auditores revisará la documentación técnica mencionada en el punto 3.1, segundo guion, para comprobar si el fabricante es capaz de identificar los requisitos pertinentes establecidos en el presente Reglamento y de efectuar los exámenes necesarios a fin de garantizar que el producto con elementos digitales cumple dichos requisitos.

La decisión se notificará al fabricante o a su representante autorizado.

La notificación incluirá las conclusiones de la auditoría y la decisión de evaluación motivada.

3.4. El fabricante se comprometerá a cumplir las obligaciones que se deriven del sistema de calidad tal como se haya aprobado y a mantenerlo de forma que siga resultando adecuado y eficaz.

3.5. El fabricante mantendrá informado al organismo notificado que haya aprobado el sistema de calidad de cualquier adaptación prevista de dicho sistema.

El organismo notificado evaluará las adaptaciones propuestas y decidirá si el sistema de calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2, o si es necesaria una nueva evaluación.

El organismo notificado notificará su decisión al fabricante. La notificación incluirá las conclusiones del examen y la decisión de evaluación motivada.

4. Supervisión bajo la responsabilidad del organismo notificado

4.1. El objetivo de la supervisión es garantizar que el fabricante cumple debidamente las obligaciones que se derivan del sistema de calidad aprobado.

4.2. El fabricante permitirá la entrada del organismo notificado en los locales de diseño, desarrollo, producción, inspección, prueba y almacenamiento, a efectos de evaluación, y le proporcionará toda la información necesaria, en particular:

– la documentación sobre el sistema de calidad,

– los registros de calidad previstos en la parte del sistema de calidad dedicada al diseño, como los resultados de análisis, cálculos y pruebas,

– los registros de calidad establecidos en la parte del sistema de calidad dedicada a la fabricación, tales como los informes de inspección, los datos sobre ensayos y calibración y los informes sobre la cualificación del personal afectado.

4.3. El organismo notificado realizará periódicamente auditorías para asegurarse de que el fabricante mantiene y aplica el sistema de calidad y proporcionará un informe de la auditoría al fabricante.

5. Marcado de conformidad y declaración de conformidad

5.1. El fabricante colocará el marcado CE y, bajo la responsabilidad del organismo notificado mencionado en el apartado 3.1, el número de identificación de este último en cada producto con elementos digitales que satisfaga los requisitos establecidos en el anexo I, parte I, del presente Reglamento.

5.2. El fabricante redactará una declaración de conformidad para cada modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada.

Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

6. El fabricante mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado:

6.1. la documentación técnica a que se refiere el punto 3.1;

6.2. la documentación relativa al sistema de calidad a que se refiere el punto 3.1;

6.3. las adaptaciones a que se refiere el punto 3.5 que hayan sido aprobadas;

6.4. las decisiones y los informes del organismo notificado a que se refieren los puntos 3.5 y 4.3.

7. Cada organismo notificado informará a sus autoridades notificantes sobre las aprobaciones de sistemas de calidad expedidas o retiradas, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de aprobaciones de sistemas de calidad que haya rechazado, suspendido o restringido de otro modo.

Cada organismo notificado informará a los demás organismos notificados sobre las aprobaciones de sistemas de calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido.

8. Representante autorizado

Las obligaciones del fabricante establecidas en los puntos 3.1, 3.5, 5 y 6 podrá cumplirlas, en su nombre y bajo su responsabilidad, su representante autorizado, siempre que las obligaciones pertinentes estén especificadas en el mandato.

En relación con el presente acto se ha formulado una declaración que se puede consultar en el … [DO: complétese la referencia al DO C , C/…,] y mediante el siguiente enlace [DO: insértese el enlace hipertexto a la declaración].