Consejo de la Unión Europea

Bruselas, 16 de septiembre de 2022
(OR. en)

12429/22

Expediente interinstitucional: 2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PROPUESTA

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	15 de septiembre de 2022
A:	Secretaría General del Consejo
N.° doc. Ción.:	COM(2022) 454 final
Asunto:	Propuesta de 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) 2019/1020

Adjunto se remite a las Delegaciones el documento – COM(2022) 454 final.

Adj.: COM(2022) 454 final

COMISIÓN
EUROPEA

Bruselas, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Propuesta de

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) 2019/1020

(Texto pertinente a efectos del EEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

Los productos consistentes en equipos informáticos (*hardware*) y en programas informáticos (*software*) están sometidos a un número cada vez mayor de ciberataques exitosos, lo que eleva el coste anual estimado de la ciberdelincuencia a 5,5 billones EUR en todo el mundo en 2021. Estos productos se enfrentan a dos problemas principales que acarrean costes adicionales para los usuarios y la sociedad: 1) un bajo nivel de ciberseguridad, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y 2) la insuficiencia de la comprensión de la información y del acceso a ella por parte de los usuarios, lo que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura. En un entorno conectado, un incidente de ciberseguridad en un producto puede afectar a toda una organización o cadena de suministro y, con frecuencia, propagarse a través de las fronteras del mercado interior en cuestión de minutos. Esto puede dar lugar a graves perturbaciones de las actividades económicas y sociales o incluso convertirse en una amenaza para la vida.

La ciberseguridad de los productos con elementos digitales tiene una importante dimensión transfronteriza, ya que los productos fabricados en un país a menudo se utilizan en todo el mercado interior. Además, es habitual que los incidentes que inicialmente afectan a una única entidad o Estado miembro se expandan en cuestión de minutos a todo el mercado interior.

Si bien la legislación vigente sobre el mercado interior se aplica a determinados productos con elementos digitales, actualmente la mayoría de los productos consistentes en equipos o programas informáticos no están contemplados en ninguna norma de la Unión Europea (UE) que regule su ciberseguridad. En particular, el marco jurídico actual de la UE no aborda la ciberseguridad de los programas informáticos no incorporados, aun cuando los ataques de ciberseguridad se centran cada vez más en las vulnerabilidades de estos productos, lo que genera considerables costes sociales y económicos. Existen numerosos ejemplos de ciberataques reseñables derivados de una seguridad insuficiente de los productos, como el programa de chantaje de tipo gusano WannaCry, que explotó una vulnerabilidad de Windows para afectar a 200 000 ordenadores en 150 países en 2017 y causó daños por valor de miles de millones de dólares estadounidenses; el ataque a la cadena de suministro de Kaseya VSA, que utilizó el programa de administración de redes de Kaseya para atacar a más de 1 000 empresas y obligó a una cadena de supermercados a cerrar la totalidad de sus 500 tiendas en Suecia; o los numerosos incidentes relacionados con el pirateo de aplicaciones bancarias para robar dinero a consumidores desprevenidos.

Se identificaron dos objetivos principales para garantizar el correcto funcionamiento del mercado interior: 1) crear condiciones 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; y 2) crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utilizar productos con elementos digitales. Se establecieron cuatro objetivos específicos: i) garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida; ii) garantizar un marco de ciberseguridad coherente y facilitar su cumplimiento por parte de los productores de equipos y programas informáticos; iii) mejorar la transparencia de las características de

seguridad de los productos con elementos digitales; y iv) permitir a las empresas y a los consumidores utilizar productos con elementos digitales de forma segura.

La importante naturaleza transfronteriza de la ciberseguridad y el aumento de los incidentes cuyas repercusiones pueden extenderse a otros países, sectores y productos hacen que los Estados miembros por sí solos no puedan alcanzar eficazmente los objetivos planteados. Habida cuenta de la dimensión mundial de los mercados de los productos con elementos digitales, los Estados miembros hacen frente en su territorio a los mismos riesgos para un mismo producto con elementos digitales. El mosaico de normas nacionales con posibles divergencias que está surgiendo corre el riesgo de poner barreras a un mercado único abierto y competitivo para los productos con elementos digitales. Por lo tanto, se hace necesaria la acción conjunta a escala de la UE para aumentar el nivel de confianza entre los usuarios y el atractivo de los productos con elementos digitales de la UE. La acción conjunta beneficiaría también al mercado interior al proporcionar seguridad jurídica y condiciones de competencia equitativas para los vendedores de productos con elementos digitales, como también se señala en el informe final de la Conferencia sobre el Futuro de Europa, en el que los ciudadanos piden reforzar el papel de la Unión en la lucha contra las amenazas a la ciberseguridad.

- **Interacción con las disposiciones existentes en la misma política sectorial**

El marco de la UE incluye varios actos legislativos horizontales que se aplican a determinados aspectos relativos a la ciberseguridad desde diferentes ángulos (productos, servicios, gestión de crisis y delitos). En 2013 entró en vigor la Directiva relativa a los ataques contra los sistemas de información[1], que armoniza la tipificación penal de una serie de delitos contra los sistemas de información y las sanciones penales aplicables. En agosto de 2016 entró en vigor la Directiva (UE) 2016/1148 sobre la seguridad de las redes y sistemas de información (Directiva SRI)[2], el primer acto legislativo a escala de la UE en materia de ciberseguridad. Su revisión, que dio origen a la Directiva [Directiva XXX/XXXX (SRI 2)], aumenta el nivel común de ambición de la UE. En 2019 entró en vigor el Reglamento sobre la Ciberseguridad de la Unión[3], que tiene por objeto mejorar la seguridad de los productos, servicios y procesos de tecnologías de la información y de las comunicaciones (TIC) mediante la introducción de un marco europeo voluntario de certificación de la ciberseguridad[4].

La ciberseguridad de toda la cadena de suministro solo está garantizada si todos sus componentes son ciberseguros. Sin embargo, la legislación de la UE mencionada anteriormente presenta carencias importantes a este respecto, ya que no establece requisitos obligatorios relativos a la seguridad de los productos con elementos digitales.

---

1 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DO L 218 de 14.8.2013, p. 8).

2 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

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 El Reglamento sobre la Ciberseguridad permite el desarrollo de esquemas de certificación específicos. Cada esquema incluye referencias a las normas, las especificaciones técnicas y otros requisitos de ciberseguridad pertinentes definidos en el esquema. La decisión de desarrollar una certificación de la ciberseguridad está basada en el riesgo.

Si bien la propuesta de Ley de Ciberresiliencia se aplica a los productos con elementos digitales que se introducen en el mercado, la Directiva [Directiva XXX/XXX (SRI 2)] tiene por objeto garantizar un elevado nivel de ciberseguridad de los servicios prestados por entidades esenciales e importantes. La Directiva [Directiva XXX/XXXX (SRI 2)] exige a los Estados miembros que garanticen que las entidades esenciales e importantes que entren en el ámbito de aplicación de la Directiva, como los proveedores de asistencia sanitaria o de servicios en nube y las entidades de la Administración pública, adoptan medidas de ciberseguridad apropiadas y proporcionadas de tipo técnico, operativo y organizativo. Estas medidas deben, entre otras cosas, garantizar la seguridad en la adquisición, el desarrollo y el mantenimiento de las redes y sistemas de información, incluidas la gestión y la divulgación de las vulnerabilidades. La Directiva [Directiva XXX/XXXX (SRI 2)] exige a la Comisión que, en un plazo de veintiún meses a partir de la fecha de entrada en vigor de la Directiva, adopte actos de ejecución que establezcan los requisitos técnicos y metodológicos de dichas medidas para determinados tipos de entidades, como los proveedores de servicios de computación en nube. Para las demás entidades, la Comisión podrá adoptar un acto de ejecución que establezca los requisitos técnicos y metodológicos, así como requisitos sectoriales. Este marco garantizará que se apliquen especificaciones y medidas técnicas similares a los requisitos esenciales de ciberseguridad de la Ley de Ciberresiliencia en lo que respecta al diseño y el desarrollo de los programas informáticos proporcionados como servicio (*software* como servicio) y la gestión de las vulnerabilidades. De este modo, se podría garantizar un elevado nivel de ciberseguridad en productos como los sistemas de historiales médicos electrónicos, en especial cuando se entregan como *software* como servicio (SaaS) o se desarrollan en instituciones sanitarias (de forma interna), de conformidad con la propuesta de [Reglamento sobre el espacio europeo de datos sanitarios].

- **Interacción con otras políticas de la Unión**

Como bien se indica en la Comunicación «Configurar el futuro digital de Europa»[5], es fundamental que la UE aproveche todas las ventajas de la era digital y que refuerce su industria y su capacidad de innovación dentro de unos límites seguros y éticos. La Estrategia Europea de Datos establece cuatro pilares (protección de datos, derechos fundamentales, seguridad y ciberseguridad) como requisitos previos esenciales para una sociedad empoderada por el uso de datos.

El marco actual de la UE[6] aplicable a los productos que también puedan tener elementos digitales está compuesto por varios actos legislativos, incluida la legislación de la UE sobre productos específicos, que regula aspectos relacionados con la seguridad y la legislación general sobre responsabilidad de los productos. La propuesta es coherente con el actual marco regulador de la UE en materia de productos, así como con ciertas propuestas legislativas recientes, como la propuesta presentada por la Comisión de Reglamento [Reglamento sobre inteligencia artificial (IA)][7].

La propuesta de Reglamento se aplicaría a todos los equipos radioeléctricos incluidos en el ámbito de aplicación del Reglamento Delegado (UE) 2022/30 de la Comisión. Además, los

---

5 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Configurar el futuro digital de Europa» [COM(2020) 67 final de 19.2.2020].

6 Principalmente la legislación relativa al nuevo marco legislativo.

7 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión [COM(2021) 206 final de 21.4.2021].

requisitos establecidos en el presente Reglamento incluyen todos los elementos de los requisitos esenciales a que se refiere el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE, incluidos los principales elementos expuestos en la [Decisión de Ejecución XXX/2022 de la Comisión relativa a una petición de normalización dirigida a las organizaciones europeas de normalización] elaborada sobre la base de dicho Reglamento Delegado. A fin de evitar un solapamiento normativo, está previsto que la Comisión derogue o modifique el Reglamento Delegado en lo que se refiere a los equipos radioeléctricos que entren en el ámbito de aplicación de la propuesta de Reglamento, de modo que sea este último el que se aplique a dichos equipos, una vez sea aplicable.

Además, para evitar la duplicación de trabajo, se prevé que la Comisión y las organizaciones europeas de normalización tengan en cuenta el trabajo de normalización llevado a cabo en el contexto de la Decisión de Ejecución C(2022)5637 de la Comisión, relativa a una petición de normalización para el Reglamento Delegado (UE) 2022/30, que completa la Directiva sobre equipos radioeléctricos, en lo que respecta a la preparación y el desarrollo de normas armonizadas para facilitar la ejecución del Reglamento.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica de la propuesta es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que trata de la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior. El objetivo de la propuesta es armonizar los requisitos de ciberseguridad de los productos con elementos digitales en todos los Estados miembros y eliminar las barreras a la libre circulación de mercancías.

El artículo 114 del TFUE puede servir como base jurídica para evitar la aparición de estas barreras, derivadas de la divergencia entre las diferentes legislaciones y enfoques nacionales en cuanto a la manera de abordar las incertidumbres jurídicas y las carencias en los marcos jurídicos existentes[8]. Además, el Tribunal de Justicia ha reconocido que la aplicación de requisitos técnicos heterogéneos podría justificar la activación del artículo 114 del TFUE[9].

El marco legislativo actual de la UE aplicable a los productos con elementos digitales se basa en el artículo 114 del TFUE y está compuesto por varios actos legislativos relativos a, entre otras cosas, productos específicos y aspectos relacionados con la seguridad, así como por legislación general sobre responsabilidad de los productos. Sin embargo, solo regula determinados aspectos relacionados con la ciberseguridad de los productos digitales tangibles y, en su caso, de los programas informáticos incorporados a estos productos. A nivel nacional, los Estados miembros están empezando a adoptar medidas nacionales que exigen a los vendedores de productos digitales la mejora de su ciberseguridad[10]. Al mismo tiempo, la ciberseguridad de los productos digitales tiene una dimensión transfronteriza de particular importancia, ya que los productos fabricados en un país suelen ser utilizados por

---

8 Sentencia del Tribunal de Justicia (Gran Sala) de 3 de diciembre de 2019, República Checa/Parlamento Europeo y Consejo de la Unión Europea, C-482/17, apartado 35.

9 Sentencia del Tribunal de Justicia (Gran Sala) de 2 de mayo de 2006, Reino Unido de Gran Bretaña e Irlanda del Norte/Parlamento Europeo y Consejo de la Unión Europea, C-217/04, apartados 62 y 63.

10 Por ejemplo, en 2019, Finlandia creó un sistema de etiquetado para dispositivos del internet de las cosas, como televisores inteligentes, teléfonos inteligentes o juguetes, sobre la base de las normas del ETSI. Alemania ha introducido recientemente una etiqueta de seguridad del consumidor para encaminadores de banda ancha, televisores inteligentes, cámaras, altavoces, juguetes y robots de limpieza y jardinería.

organizaciones y consumidores en todo el mercado interior. Los incidentes que inicialmente afectan a una única entidad o Estado miembro a menudo se propagan en cuestión de minutos a otras organizaciones, sectores y Estados miembros.

Los diversos actos e iniciativas adoptados hasta la fecha a escala nacional y de la UE abordan solo de manera parcial los problemas detectados, por lo que se corre el riesgo de crear un mosaico legislativo en el mercado interior, aumentar la inseguridad jurídica tanto para los vendedores como para los usuarios de estos productos y añadir una carga innecesaria a las empresas vinculada al cumplimiento de una serie de requisitos para tipos similares de productos.

El Reglamento propuesto armonizaría y racionalizaría el panorama normativo de la UE mediante la introducción de requisitos de ciberseguridad para los productos con elementos digitales y evitaría el solapamiento de requisitos establecidos en diferentes actos legislativos. La adopción de este Reglamento favorecería una mayor seguridad jurídica para los operadores y los usuarios de toda la Unión, así como una mejor armonización del mercado único europeo, y establecería condiciones más viables para los operadores que desearan acceder al mercado de la UE.

- **Subsidiariedad (en el caso de competencia no exclusiva)**

La importante naturaleza transfronteriza de la ciberseguridad en general y el aumento de los riesgos e incidentes, cuyas repercusiones pueden extenderse a otros países, sectores y productos, hacen que los Estados miembros por sí solos no puedan alcanzar eficazmente los objetivos de la presente intervención. Los enfoques nacionales para abordar los problemas, en particular los que introducen requisitos obligatorios, generarán una mayor inseguridad jurídica y obstáculos jurídicos adicionales. También podrían impedir a las empresas expandirse sin trabas a otros Estados miembros, privando así a los usuarios de los beneficios de sus productos.

Es por tanto necesaria la acción conjunta a escala de la UE para establecer un elevado nivel de confianza entre los usuarios y aumentar el atractivo de los productos con elementos digitales de la UE. La acción conjunta también beneficiaría al mercado único digital y al mercado interior en general al proporcionar seguridad jurídica y condiciones de competencia equitativas para los fabricantes de productos con elementos digitales.

En última instancia, las Conclusiones del Consejo, de 23 de mayo de 2022, sobre el desarrollo de la posición de la Unión Europea en materia de ciberseguridad, piden a la Comisión que, a más tardar a finales de 2022, proponga requisitos comunes de ciberseguridad para los dispositivos conectados.

- **Proporcionalidad**

Por lo que respecta a la proporcionalidad del Reglamento propuesto, las medidas incluidas en las opciones de actuación planteadas no rebasarían los límites estrictamente necesarios para lograr los objetivos generales y específicos y no impondrían costes desproporcionados. Más concretamente, la intervención planteada garantizaría que los productos con elementos digitales estuvieran protegidos a lo largo de todo su ciclo de vida, de forma proporcional a los riesgos presentes, mediante requisitos orientados a objetivos, tecnológicamente neutros, de un alcance razonable y, en general, coherentes con los intereses de las entidades implicadas.

Los requisitos esenciales de ciberseguridad propuestos se basan en normas de uso generalizado, y el proceso de normalización subsecuente tendría en cuenta las especificidades técnicas de los productos. Esto supone que los controles de seguridad se adaptarían cuando un determinado nivel de riesgo así lo requiriera. Además, las normas horizontales previstas solo

contemplarían las evaluaciones de terceros para los productos críticos. Esto solo afectaría a una pequeña parte del mercado de los productos con elementos digitales. Las repercusiones en las pymes dependerían de su presencia en el mercado de estas categorías específicas de productos.

En cuanto a la proporcionalidad de los costes de la evaluación de la conformidad, los organismos notificados que llevaran a cabo las evaluaciones de terceros tendrían en cuenta el tamaño de la empresa a la hora de fijar las tasas aplicables. También se establecería un período de transición razonable de veinticuatro meses para preparar la ejecución, a fin de dar tiempo a los mercados pertinentes para que se preparen y, al mismo tiempo, proporcionar directrices claras para las inversiones en I+D. Los costes de cumplimiento para las empresas se verían compensados con creces por los beneficios que les reportaría un nivel de seguridad más elevado de los productos con elementos digitales y, en última instancia, un aumento de la confianza de los usuarios en estos productos.

- **Elección del instrumento**

Una intervención reguladora implicaría la adopción de un reglamento y no de una directiva. Esto se debe a que, para este tipo concreto de legislación sobre productos, un reglamento abordaría los problemas detectados y cumpliría los objetivos formulados con mayor eficacia, ya que se trata de una intervención que condiciona la comercialización en el mercado interior de una categoría muy amplia de productos. Para este tipo de intervención, el proceso de transposición en el caso de una directiva podría dejar un margen de discrecionalidad a nivel nacional demasiado amplio, lo que podría dar lugar a una falta de homogeneidad de determinados requisitos esenciales de ciberseguridad, inseguridad jurídica, una mayor fragmentación del mercado o incluso situaciones discriminatorias a nivel transfronterizo, más aún teniendo en cuenta que los productos afectados pueden tener múltiples fines o usos y que los fabricantes pueden producir múltiples categorías de estos productos.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Consultas con las partes interesadas**

La Comisión ha consultado a un amplio abanico de partes interesadas. Se invitó a los Estados miembros y a las partes interesadas a participar en la consulta pública abierta y en las encuestas y talleres organizados en el marco de un estudio realizado por un consorcio que apoya a la Comisión en sus trabajos preparatorios para la evaluación de impacto, formado por Wavestone, el Centro de Estudios Políticos Europeos (CEPS) e ICF. Entre las partes interesadas consultadas figuraban autoridades nacionales de vigilancia del mercado, órganos de la Unión cuyo trabajo se enmarca en el ámbito de la ciberseguridad, fabricantes de equipos y programas informáticos, importadores y distribuidores de equipos y programas informáticos, asociaciones comerciales, organizaciones de consumidores y usuarios de productos con elementos digitales, ciudadanos, investigadores y representantes del mundo académico, organismos notificados y de acreditación y profesionales del sector de la ciberseguridad.

Estas fueron las actividades de consulta:

- Un estudio inicial realizado por un consorcio formado por ICF, Wavestone, Carsa y el CEPS, publicado en diciembre de 2021[11]. El estudio detectó varias deficiencias del mercado y evaluó posibles intervenciones reguladoras.
- Una consulta pública abierta dirigida a los ciudadanos, las partes interesadas y expertos en ciberseguridad. Se recibieron 176 respuestas, que contribuyeron a la recopilación de opiniones y experiencias diversas de todos los grupos de partes interesadas.
- Talleres organizados en el marco del estudio que apoyó los trabajos preparatorios de la Comisión para una Ley de Ciberresiliencia, que reunieron a unos cien representantes de diversas partes interesadas de los veintisiete Estados miembros.
- Entrevistas con expertos realizadas con el objetivo de comprender mejor los retos actuales en materia de ciberseguridad que afectan a los productos con elementos digitales y debatir opciones de actuación para una posible intervención normativa.
- Debates bilaterales con las autoridades nacionales de ciberseguridad, el sector privado y las organizaciones de consumidores.
- Un acercamiento específico a las principales partes interesadas en el ámbito de las pymes.

- **Obtención y utilización de asesoramiento técnico**

Las actividades de consulta tenían por objeto obtener aportaciones sobre los cinco criterios de evaluación principales, basados en las directrices de la UE para la mejora de la legislación (eficacia, eficiencia, pertinencia, coherencia, valor añadido de la UE), así como sobre las repercusiones potenciales de las posibles opciones para el futuro. El contratista no solo se ha puesto en contacto con las partes interesadas a las que el Reglamento propuesto afectaría directamente, sino que también ha consultado a una amplia gama de expertos en el ámbito de la ciberseguridad.

- **Evaluación de impacto**

La Comisión sometió la presente propuesta a una evaluación de impacto que fue examinada por su Comité de Control Reglamentario. El 6 de julio de 2022 se celebró una reunión con dicho Comité, que al término de esta emitió un dictamen positivo. La evaluación de impacto se ajustó para tener en cuenta las recomendaciones y observaciones del Comité.

La Comisión examinó diversas opciones de actuación para alcanzar el objetivo general de la propuesta:

- Enfoque de Derecho indicativo y medidas voluntarias (opción 1): en esta opción no se llevaría a cabo ninguna intervención normativa obligatoria. En su lugar, la Comisión publicaría comunicaciones, orientaciones, recomendaciones y, dado el caso, códigos de conducta para fomentar la adopción de medidas voluntarias. Los regímenes nacionales, ya fueran voluntarios u obligatorios,

[11] *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715, Final Study Report* [«Estudio sobre la necesidad de requisitos de ciberseguridad para los productos de TIC; N.º 2020-0715, Informe final del estudio», documento en inglés], disponible en https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

seguirían desarrollándose para compensar la ausencia de normas horizontales de la UE.

- Intervención normativa *ad hoc* para la ciberseguridad de los productos tangibles con elementos digitales y sus respectivos programas informáticos incorporados (opción 2): esta opción implicaría una intervención normativa *ad hoc* específica del producto que se limitaría a añadir o modificar los requisitos de ciberseguridad en la legislación ya existente o a introducir nueva legislación a medida que surgieran nuevos riesgos, incluidos los que afecten a los programas informáticos no incorporados.

Las opciones 3 y 4 implican una intervención normativa horizontal de alcance variable, derivada en gran medida del nuevo marco legislativo. Este marco establece una serie de requisitos esenciales como condición para la introducción de determinados productos en el mercado interior. El nuevo marco legislativo también suele prever una evaluación de la conformidad, que es el proceso que el fabricante lleva a cabo para demostrar que se han cumplido los requisitos específicos relativos a un producto.

- Enfoque mixto que incluya normas horizontales obligatorias para la ciberseguridad de los productos tangibles con elementos digitales y sus respectivos programas informáticos incorporados y un enfoque escalonado para los programas informáticos no incorporados (opción 3): esta opción incluiría un reglamento que introduciría requisitos horizontales de ciberseguridad para todos los productos tangibles con elementos digitales, así como para los programas informáticos incorporados en ellos, como condición para su introducción en el mercado, y contaría con dos subopciones según la obligatoriedad o no de la evaluación de terceros (3i y 3ii). Los programas informáticos no incorporados no estarían regulados.
- Intervención normativa horizontal que introduzca requisitos de ciberseguridad para una amplia gama de productos tangibles e intangibles con elementos digitales, incluidos los programas informáticos no incorporados (opción 4): esta opción es similar a la opción 3, excepto por el ámbito de aplicación. La opción 4 incluiría los programas informáticos no incorporados [con dos subopciones que incluirían, respectivamente, únicamente los programas críticos (4a) o todos los programas (4b)] en el ámbito de aplicación de un posible reglamento. Para cada subopción, se contemplarían las mismas subopciones relativas a la evaluación de la conformidad que en la opción 3.

La opción 4 (con las subopciones que abarcan todos los programas informáticos e implican una evaluación de terceros obligatoria para los productos críticos) se posicionó como la opción preferida sobre la base de la evaluación de la eficacia respecto de los objetivos específicos y la eficiencia entre costes y beneficios. Esta opción garantizaría el establecimiento de requisitos horizontales de ciberseguridad específicos para todos los productos con elementos digitales que se introduzcan o comercialicen en el mercado interior y sería la única opción que abarcaría toda la cadena de suministro digital. Los programas informáticos no incorporados, a menudo expuestos a vulnerabilidades, también estarían cubiertos por esta intervención normativa, lo que garantizaría un enfoque coherente respecto de todos los productos con elementos digitales y posibilitaría un reparto claro de responsabilidades entre los distintos operadores económicos.

Esta opción también aporta valor añadido al cubrir aspectos relacionados con el deber de diligencia y el ciclo de vida completo tras la introducción en el mercado de los productos con elementos digitales, a fin de garantizar, entre otras cosas, el suministro de actualizaciones de

seguridad e información adecuada sobre el apoyo en materia de seguridad. Esta opción también sería la que complementaría de la manera más eficaz la reciente revisión del marco SRI, ya que garantizaría el establecimiento de condiciones previas para reforzar la seguridad de la cadena de suministro.

La opción preferida beneficiaría considerablemente a las distintas partes interesadas. Por lo que respecta a las empresas, evitaría la divergencia entre las normas de seguridad para los productos con elementos digitales y reduciría los costes de cumplimiento de la legislación pertinente en materia de ciberseguridad. Reduciría el número de ciberincidentes, los costes de gestión de incidentes y el daño a la reputación. Para el conjunto de la UE, se calcula que la iniciativa podría dar lugar a una reducción de los costes derivados de los incidentes que afectan a las empresas de entre 180 000 y 290 000 millones EUR anuales aproximadamente. Esto permitiría un aumento del consumo de productos con elementos digitales y, por tanto, del volumen de negocio. También mejoraría la reputación mundial de las empresas, lo que a su vez daría lugar a un aumento de la demanda también fuera de la UE. A nivel de los usuarios, la opción preferida aumentaría la transparencia de las propiedades de seguridad y facilitaría el uso de productos con elementos digitales. Los consumidores y los ciudadanos también se beneficiarían de una mejor protección de sus derechos fundamentales, como la privacidad y la protección de datos.

Al pedírseles que evaluaran la eficacia de las intervenciones políticas, los participantes en la consulta pública coincidieron en que la opción 4 sería la medida más eficaz (4,08 en una escala de 1 a 5). Aquí se incluyen las valoraciones de las organizaciones de consumidores (5,00), los encuestados que se identifican como usuarios (4,22), los organismos notificados (4,17), las autoridades de vigilancia del mercado (5,00) y los productores de productos con elementos digitales (3,85), incluidas las pymes (4,05).

- **Adecuación y simplificación normativa**

La presente propuesta establece los requisitos que se aplicarán a los fabricantes de equipos y programas informáticos. Es necesario garantizar la seguridad jurídica y evitar una mayor fragmentación del mercado con respecto a los requisitos de ciberseguridad para los productos en el mercado interior, lo que ha quedado demostrado por el amplio apoyo de las diversas partes interesadas a una intervención horizontal. La propuesta reducirá al mínimo la carga normativa para los fabricantes que tienen que manejar varios instrumentos legislativos aplicables a la seguridad de sus productos. La alineación con el nuevo marco legislativo supone un mejor funcionamiento de la intervención y su ejecución. La propuesta racionaliza el proceso de los procedimientos de salvaguardia involucrando a los fabricantes y a los Estados miembros antes de la notificación a la Comisión. Gran parte de los fabricantes que entran en el ámbito de aplicación de la propuesta ya están familiarizados con el funcionamiento del nuevo marco legislativo, lo que contribuirá a su comprensión y ejecución. La propuesta también promoverá la confianza de los consumidores y las empresas en los productos con elementos digitales.

- **Derechos fundamentales**

Se espera que todas las opciones de actuación mejoren en cierta medida la protección de los derechos y las libertades fundamentales, como la privacidad, la protección de los datos personales, la libertad de empresa y la protección de los bienes y de la dignidad y la integridad de las personas. En particular, la opción 4 preferida, consistente en intervenciones normativas horizontales y un ámbito de actuación amplio, sería la más eficaz a este respecto, puesto que es más probable que contribuya a reducir el número y la gravedad de los incidentes, incluidas las violaciones de la seguridad de los datos personales. También

reforzaría la seguridad jurídica, establecería unas condiciones de competencia equitativas para los operadores económicos y aumentaría la confianza de los usuarios y el atractivo de los productos de la UE con elementos digitales en su conjunto, lo que mejoraría la protección de los bienes y las condiciones para que los operadores económicos ejerzan actividades empresariales.

Los requisitos horizontales de ciberseguridad contribuirían a la seguridad de los datos personales al proteger la confidencialidad, la integridad y la disponibilidad de información en los productos con elementos digitales. El cumplimiento de estos requisitos facilitaría a su vez el cumplimiento del requisito de seguridad del tratamiento de los datos personales en virtud del Reglamento (UE) 2016/679 (Reglamento general de protección de datos)[12]. La propuesta mejoraría la transparencia y la información para los usuarios, en especial aquellos que pudieran estar menos capacitados en materia de ciberseguridad. Los usuarios también estarían mejor informados acerca de los riesgos, las capacidades y las limitaciones de los productos con elementos digitales y, por tanto, mejor preparados para adoptar las medidas preventivas y paliativas necesarias a fin de reducir los riesgos residuales.

4. REPERCUSIONES PRESUPUESTARIAS

A fin de cumplir las tareas asignadas a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en virtud del mencionado Reglamento, la ENISA tendrá que reasignar unos recursos aproximados de 4,5 EJC. La Comisión tendría que asignar 7 EJC para hacer frente a las responsabilidades en materia de ejecución que le atribuiría el Reglamento.

En la «ficha financiera» vinculada a esta propuesta se ofrece una descripción detallada de los costes.

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

La Comisión hará un seguimiento de la ejecución, la aplicación y el cumplimiento de estas nuevas disposiciones con miras a evaluar su eficacia. El Reglamento solicitará una evaluación y revisión por parte de la Comisión y la presentación de un informe público a este respecto al Parlamento Europeo y al Consejo a más tardar treinta y seis meses después de su fecha de aplicación, y posteriormente cada cuatro años.

- **Explicación detallada de las disposiciones específicas de la propuesta**

Disposiciones generales (capítulo I)

La presente propuesta de Reglamento establece: a) normas para la introducción en el mercado de productos con elementos digitales destinadas a garantizar la ciberseguridad de dichos productos; b) requisitos esenciales para el diseño, el desarrollo y la fabricación de productos con elementos digitales y las obligaciones de los operadores económicos en relación con dichos productos respecto de la ciberseguridad; c) requisitos esenciales para los procesos de gestión de las vulnerabilidades establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales a lo largo de todo el ciclo de vida y

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

las obligaciones de los operadores económicos en relación con dichos procesos; d) normas relativas a la vigilancia del mercado y a la aplicación de los requisitos y las normas antes mencionados.

El Reglamento propuesto se aplicará a todos los productos con elementos digitales cuyo uso previsto y razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

El Reglamento propuesto no se aplicará a los productos con elementos digitales que entren en el ámbito de aplicación del Reglamento (UE) 2017/745 [productos sanitarios para uso humano y accesorios de dichos productos] y del Reglamento (UE) 2017/746 [productos sanitarios para diagnóstico *in vitro* de uso humano y accesorios de dichos productos], ya que ambos Reglamentos contienen requisitos relativos a los productos, incluidos los programas informáticos y las obligaciones generales de los fabricantes, que abarcan todo el ciclo de vida de los productos, así como procedimientos de evaluación de la conformidad. El presente Reglamento no se aplicará a los productos con elementos digitales que hayan sido certificados de conformidad con el Reglamento 2018/1139 [nivel elevado y uniforme de seguridad de la aviación civil], ni a los productos regulados por el Reglamento (UE) 2019/2144 [relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos].

Los productos críticos con elementos digitales estarán sujetos a procedimientos específicos de evaluación de la conformidad y se dividirán en las clases I y II según lo establecido en el anexo III, dependiendo de su nivel de riesgo de ciberseguridad, conforme al que la clase II presenta un riesgo más elevado. Un producto con elementos digitales se considera crítico y, por tanto, se incluye en el anexo III considerando las repercusiones de las posibles vulnerabilidades de ciberseguridad presentes en el producto con elementos digitales. A la hora de determinar el riesgo de ciberseguridad se tienen en cuenta la funcionalidad del producto con elementos digitales relacionada con la ciberseguridad y el uso previsto del producto en entornos sensibles, como, entre otros, el industrial.

La Comisión también estará facultada para adoptar actos delegados que completen el presente Reglamento mediante el establecimiento de categorías de productos altamente críticos con elementos digitales, a cuyos fabricantes se debe exigir la obtención de un certificado europeo de ciberseguridad expedido en el marco de un esquema europeo de certificación de la ciberseguridad, a fin de demostrar la conformidad con los requisitos esenciales establecidos en el anexo I o parte de ellos. Para determinar estas categorías de productos altamente críticos con elementos digitales, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad vinculado a cada categoría de productos con elementos digitales, a la luz de uno o varios de los criterios tomados en consideración para la inclusión de productos críticos con elementos digitales en el anexo III, así como de la evaluación que determine si dicha categoría de productos es utilizada por las entidades esenciales del tipo contemplado en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)], si sirve a estas entidades de referencia o si, en el futuro, podría desempeñar un papel importante para sus actividades; o bien si resulta pertinente para la resiliencia de la cadena de suministro global de productos con elementos digitales frente a las perturbaciones.

Obligaciones de los operadores económicos (capítulo II)

La propuesta incorpora obligaciones para los fabricantes, importadores y distribuidores sobre la base de las disposiciones de referencia previstas en la Decisión 768/2008/CE. Los requisitos y obligaciones esenciales de ciberseguridad exigen que los productos con elementos digitales solo se comercialicen si, habiendo sido suministrados debidamente, instalados de manera adecuada, mantenidos y utilizados para los fines previstos, o en condiciones de uso

que se puedan prever razonablemente, cumplen los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento.

Los requisitos y obligaciones esenciales obligarían a los fabricantes a tener en cuenta la ciberseguridad en el diseño, el desarrollo y la producción de los productos con elementos digitales, a actuar con la diligencia debida en lo que respecta a la seguridad al diseñar y desarrollar sus productos, a ser transparentes con respecto a los aspectos relativos a la ciberseguridad que deban ponerse en conocimiento de los clientes, a garantizar el apoyo en materia de seguridad (actualizaciones) de manera proporcionada y a cumplir los requisitos relacionados con la gestión de las vulnerabilidades.

Se establecerían también obligaciones para los operadores económicos, desde los fabricantes hasta los distribuidores y los importadores, relativas a la introducción en el mercado de productos con elementos digitales, conformemente a su papel y sus responsabilidades en la cadena de suministro.

Conformidad del producto con elementos digitales (capítulo III)

Se presupondrá que los productos con elementos digitales 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 del Reglamento propuesto. Cuando no existan normas armonizadas o sean insuficientes, cuando se produzcan retrasos indebidos en el procedimiento de normalización o cuando la solicitud de la Comisión no haya sido aceptada por los organismos europeos de normalización, la Comisión podrá, mediante actos de ejecución, adoptar especificaciones comunes.

Además, se presumirá que los productos con elementos digitales que hayan sido certificados o para los que se haya expedido una declaración de conformidad de la UE o un certificado en el marco de un esquema europeo de certificación de la ciberseguridad establecido en virtud del Reglamento (UE) 2019/881 y para los cuales la Comisión haya especificado, mediante acto de ejecución, que puede otorgar la presunción de conformidad con el Reglamento propuesto son conformes con los requisitos esenciales del presente Reglamento o partes de estos, en la medida en que la declaración de conformidad de la UE o el certificado de ciberseguridad, o partes de estos, contemplen dichos requisitos.

Además, con el fin de evitar cargas administrativas excesivas para los fabricantes, la Comisión debe, cuando proceda, especificar si un certificado de ciberseguridad expedido en el marco de uno de estos esquemas europeos de certificación de la ciberseguridad elimina la obligación 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.

El fabricante llevará a cabo una evaluación de la conformidad del producto con elementos digitales y los procesos de gestión de las vulnerabilidades que haya establecido para demostrar la conformidad con los requisitos esenciales establecidos en el anexo I por medio de uno de los procedimientos establecidos en el anexo VI. Los fabricantes de productos críticos de las clases I y II utilizarán los módulos respectivos necesarios para su cumplimiento. Los fabricantes de productos críticos de la clase II deberán recurrir a un tercero para su evaluación de la conformidad.

Notificación de los organismos de evaluación de la conformidad (capítulo IV)

El funcionamiento adecuado de los organismos notificados es crucial para garantizar un nivel elevado de ciberseguridad y para que todas las partes interesadas confíen en el sistema del nuevo enfoque. Por tanto, en sintonía con la Decisión 768/2008/CE, la propuesta establece los requisitos aplicables a las autoridades nacionales responsables de los organismos de evaluación de la conformidad (organismos notificados). Deja en manos de los Estados

miembros la responsabilidad final de la designación y la supervisión de los organismos notificados. Los Estados miembros designarán a una autoridad notificante que será responsable de establecer y aplicar los procedimientos necesarios para la evaluación y notificación de los organismos de evaluación de la conformidad y para la supervisión de los organismos notificados.

Vigilancia del mercado y aplicación de la legislación (capítulo V)

De conformidad con el Reglamento (UE) 2019/1020, las autoridades nacionales de vigilancia del mercado son responsables de efectuar la vigilancia del mercado en el territorio de ese Estado miembro. Los Estados miembros podrán 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 a que se refiere el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] y las autoridades nacionales de certificación de la ciberseguridad designadas a que se refiere el artículo 58 del Reglamento (UE) 2019/881. Se pide a los operadores económicos que cooperen plenamente con las autoridades de vigilancia del mercado y otras autoridades competentes.

Poderes delegados y procedimientos de comité (capítulo VI)

A fin de garantizar que el marco regulador pueda adaptarse cuando sea necesario, se delegan en la Comisión los poderes para adoptar actos con arreglo a lo dispuesto en el artículo 290 del TFUE a efectos de: actualizar la lista de productos críticos de las clases I y II y especificar las definiciones de dichos productos, especificar si es necesario limitar o excluir los productos con elementos digitales regulados por otras normas de la Unión que establecen requisitos con el mismo nivel de protección que el presente Reglamento, exigir la certificación de determinados productos altamente críticos con elementos digitales sobre la base de los criterios establecidos en el presente Reglamento, especificar el contenido mínimo de la declaración de conformidad de la UE y completar los elementos que deban incluirse en la documentación técnica.

La Comisión también estará facultada para adoptar actos de ejecución con el fin de: especificar el formato o los elementos de los informes obligatorios y la nomenclatura de materiales de los programas informáticos, especificar los esquemas europeos de certificación de la ciberseguridad que puedan utilizarse para demostrar la conformidad con los requisitos esenciales o partes de estos establecidos en el presente Reglamento, adoptar especificaciones comunes, establecer especificaciones técnicas para la colocación del marcado CE y adoptar medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata destinada a preservar el buen funcionamiento del mercado interior.

Confidencialidad y sanciones (capítulo VII)

Todas las partes que apliquen el presente Reglamento respetarán la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones y actividades.

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. En la misma línea, el presente Reglamento establece los niveles máximos para las multas administrativas que deben recoger las legislaciones nacionales para casos de incumplimiento de las obligaciones establecidas en el presente Reglamento.

Disposiciones transitorias y finales (capítulo VIII)

Para que los fabricantes, los organismos notificados y los Estados miembros dispongan de tiempo suficiente para adaptarse a los nuevos requisitos, el Reglamento propuesto será aplicable [veinticuatro meses] después de su entrada en vigor, a excepción de la obligación de información de los fabricantes, que se aplicaría [doce meses] después de la fecha de entrada en vigor.

2022/0272 (COD)

Propuesta de

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) 2019/1020

(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],

Visto el dictamen del Comité de las Regiones[2],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Es necesario mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la comercialización de productos con elementos digitales en 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.

(3) La legislación pertinente de la Unión actualmente en vigor está compuesta 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, la legislación vigente de la

[1] DO C […] de […], p. […].
[2] DO C […] de […], p. […].

Unión relativa a la ciberseguridad, en particular la [Directiva XXX/XXXX (SRI 2)] y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[3], no aborda de manera directa los requisitos obligatorios para la seguridad de los productos con elementos digitales.

(4) Aunque la legislación 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 vinculada al cumplimiento de una serie de requisitos para tipos de productos similares. La ciberseguridad de estos productos tiene una dimensión transfronteriza de particular importancia, ya que los productos fabricados en un país 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. El panorama normativo de la Unión debe armonizarse mediante la introducción de requisitos de ciberseguridad para los productos con elementos digitales. Además, debe garantizarse una mayor seguridad jurídica para los operadores y los usuarios de toda la Unión, así como una mejor armonización del mercado único, y de este modo establecer condiciones más viables para los operadores que deseen acceder al mercado de la Unión.

(5) A escala de la Unión, diversos documentos programáticos y políticos, como la Estrategia de Ciberseguridad de la UE para la Década Digital[4], las Conclusiones del Consejo de 2 de diciembre de 2020 y de 23 de mayo de 2022 o la Resolución del Parlamento Europeo de 10 de junio de 2021[5], han hecho un llamamiento a que se establezcan requisitos específicos de ciberseguridad de la Unión para los productos digitales o conectados, y varios países de todo el mundo han introducido por iniciativa propia medidas para abordar esta cuestión. En el informe final de la Conferencia sobre el Futuro de Europa[6], los ciudadanos pidieron «reforzar el papel de la Unión en la lucha contra las amenazas a la ciberseguridad».

(6) 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 estos productos.

(7) 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

---

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 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_ES.html.

6 «Conferencia sobre el Futuro de Europa. Informe sobre el resultado final», mayo de 2022, propuesta 28, punto 2. La Conferencia se celebró entre abril de 2021 y mayo de 2022. Fue un ejercicio único, dirigido por los ciudadanos, de democracia deliberativa a nivel paneuropeo, en el que participaron miles de ciudadanos europeos, así como agentes políticos, interlocutores sociales, representantes de la sociedad civil y partes interesadas clave.

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 conectables se diseñen y desarrollen de conformidad con los requisitos esenciales establecidos en el presente Reglamento. Se incluyen aquí 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 aquellos productos cuya conexión a otros dispositivos o redes es indirecta.

(8) El establecimiento de requisitos de ciberseguridad para la introducción en el mercado de productos con elementos digitales mejorará la ciberseguridad de dichos productos tanto para los consumidores como para las empresas. 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 vigilabebés.

(9) El presente Reglamento garantiza un elevado nivel de ciberseguridad de los productos con elementos digitales. No regula servicios, como el *software* como servicio (SaaS), excepto en el caso de las soluciones de tratamiento de datos a distancia relacionadas con un producto con elementos digitales, entendido como todo tratamiento de datos a distancia para el que el programa informático haya sido diseñado y desarrollado por el fabricante del producto en cuestión o bajo la responsabilidad de dicho fabricante, y cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones. La [Directiva XXX/XXXX (SRI 2)] establece requisitos de ciberseguridad y de notificación de incidentes para las entidades esenciales e importantes, como las infraestructuras críticas, con el objetivo de aumentar la resiliencia de los servicios prestados. La [Directiva XXX/XXXX (SRI 2)] se aplica a los servicios de computación en nube y a los modelos de servicios en nube, como el SaaS. Todas las entidades que prestan servicios de computación en nube en la Unión y alcanzan o superan el umbral para las medianas empresas entran en el ámbito de aplicación de la Directiva.

(10) Para no obstaculizar la innovación o la investigación, el presente Reglamento no debe aplicarse a los programas informáticos libres y de código abierto desarrollados o suministrados al margen de una actividad comercial. Este es el caso, en particular, de los programas informáticos, incluidos su código fuente y sus versiones modificadas, que se comparten abiertamente y son accesibles, utilizables, modificables y redistribuibles libremente. En el contexto de los programas informáticos, una actividad comercial puede caracterizarse no solo por la aplicación de un precio a un producto, sino también por la aplicación de un precio a los servicios de asistencia técnica, por el suministro de una plataforma de *software* a través de la cual el fabricante monetiza otros servicios o por el uso de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático.

(11) Una internet segura es indispensable para el funcionamiento de las infraestructuras críticas y para la sociedad en su conjunto. La [Directiva XXX/XXXX (SRI 2)] tiene

por objeto garantizar un elevado nivel de ciberseguridad de los servicios prestados por entidades esenciales e importantes, incluidos los proveedores de infraestructuras digitales que apoyan las funciones básicas de la internet abierta o garantizan el acceso a internet y 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 XXX/XXXX (SRI 2)], 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.

(12) El Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo[7] establece normas sobre los productos sanitarios y el Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo[8] establece normas sobre los productos sanitarios para diagnóstico *in vitro*. Ambos 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 para los productos sanitarios que funcionan a través de un sistema electrónico o que son en sí mismos programas informáticos. Estos Reglamentos también abarcan algunos tipos de programas informáticos no incorporados y el enfoque global del ciclo de vida. Estos 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 pertinentes relativos a la ciberseguridad establecidos en el anexo I de dichos Reglamentos[9]. Por lo tanto, los productos con elementos digitales a los que se aplique alguno de estos Reglamentos no deben estar sujetos al presente Reglamento.

(13) El Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo[10] establece requisitos para la homologación de tipo de los vehículos, así como de sus sistemas y

---

7 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).

8 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).

9 MDCG 2019-16, aprobado por el Grupo de Coordinación de Productos Sanitarios (MDCG) que se estableció en virtud del artículo 103 del Reglamento (UE) 2017/745.

10 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)

componentes, a cuyo fin introduce determinados requisitos de ciberseguridad, en particular 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[11]; y establece procedimientos específicos de evaluación de la conformidad. 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 aeronavegabilidad de los productos, componentes y equipos aeronáuticos, incluidos los programas informáticos, en el que se tienen en cuenta las obligaciones relativas a la protección contra las amenazas para la seguridad de la información. 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 están sujetos a los requisitos esenciales ni a los procedimientos de evaluación de la conformidad establecidos en el presente Reglamento. El proceso de certificación establecido en el Reglamento (UE) 2018/1139 garantiza el nivel de garantía al que aspira el presente Reglamento.

(14) 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 establecidos en el presente Reglamento. En tales casos, la aplicación del presente Reglamento a los productos con elementos digitales sujetos a otras normas de la Unión que establezcan requisitos que abordan la totalidad o parte de los riesgos cubiertos por los requisitos esenciales establecidos en el anexo I del presente Reglamento podrá 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 un nivel de protección equivalente al previsto en el presente Reglamento. La Comisión estará facultada para adoptar actos delegados a fin de modificar el presente Reglamento mediante la especificación de dichos productos y normas. El presente Reglamento contiene disposiciones específicas que aclaran su relación con la legislación vigente de la Unión que implique la aplicación de tales limitaciones o exclusiones.

---

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).

11 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 [2021/387].

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).

(15) El Reglamento Delegado (UE) 2022/30 especifica que los requisitos esenciales establecidos en el artículo 3, apartado 3, letra d) (daños a la red y utilización inadecuada de los recursos de la red), letra e) (datos personales y privacidad) y letra f) (fraude) de la Directiva 2014/53/UE se aplican a determinados equipos radioeléctricos. [La Decisión de Ejecución XXX/2022 de la Comisión relativa a una petición de normalización dirigida a las organizaciones europeas de normalización] establece requisitos para la elaboración de normas específicas que detallan con mayor precisión cómo deben abordarse estos tres requisitos esenciales. Los requisitos esenciales establecidos por el presente Reglamento incluyen todos los elementos de los requisitos esenciales mencionados en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE. Además, los requisitos esenciales 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, si 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 de la Comisión, relativa a una petición de normalización para el Reglamento Delegado (UE) 2022/30, que completa la Directiva sobre equipos radioeléctricos, en lo que respecta a la preparación y el desarrollo de normas armonizadas para facilitar la ejecución del presente Reglamento.

(16) La Directiva 85/374/CEE[13] se complementa con el presente Reglamento. Esta 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.

(17) El presente Reglamento debe entenderse sin perjuicio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[14], en particular de las disposiciones para implantar 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

[13] Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (DO L 210 de 7.8.85).

[14] 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).

personales y la privacidad de las personas. Deben tenerse en cuenta las sinergias tanto en materia de normalización como de certificación en 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 (CEPD) 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 en virtud del presente Reglamento deben cooperar con las autoridades responsables de la supervisión 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.

(18) En la medida en que sus productos entren en el ámbito de aplicación del presente Reglamento, los emisores de carteras de identidad digital europea a que se refiere el artículo [artículo 6 *bis*, apartado 2, del Reglamento (UE) n.º 910/2014, modificado por la propuesta de Reglamento por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea] deben cumplir tanto los requisitos esenciales horizontales establecidos en el presente Reglamento como los requisitos específicos de seguridad establecidos en el artículo [artículo 6 *bis* del Reglamento (UE) n.º 910/2014, modificado por la propuesta de Reglamento por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea]. A fin de facilitar el cumplimiento de sus obligaciones, los emisores de carteras deben poder demostrar la conformidad de las carteras de identidad digital europea con los requisitos establecidos en cada uno de los dos actos mediante la certificación de sus productos con arreglo a un esquema europeo de certificación de la ciberseguridad establecido en virtud del Reglamento (UE) 2019/881 para el cual la Comisión haya especificado, mediante acto de ejecución, una presunción de conformidad con el presente Reglamento, en la medida en que el certificado, o partes de este, abarque dichos requisitos.

(19) De conformidad con el artículo 3, apartado 2, del Reglamento (UE) 2019/881, corresponde a la ENISA desempeñar determinadas tareas previstas en el presente Reglamento. En particular, la ENISA debe recibir notificaciones de los fabricantes relativas a las vulnerabilidades aprovechadas activamente presentes en los productos con elementos digitales y a los incidentes que repercutan en la seguridad de dichos productos. La ENISA también debe transmitir estas notificaciones a los equipos de respuesta a incidentes de seguridad informática (CSIRT) pertinentes o, según corresponda, a los puntos de contacto únicos de los Estados miembros designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como informar a las autoridades de vigilancia del mercado pertinentes sobre la vulnerabilidad notificada. 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 especificado en la Directiva [Directiva XXX/XXXX (SRI 2)]. Además, teniendo en cuenta sus conocimientos técnicos y su mandato, la ENISA debe poder apoyar el proceso de ejecución del presente Reglamento. En particular, debe ser capaz de proponer actividades conjuntas que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre el posible incumplimiento del presente Reglamento por parte de productos con

elementos digitales en varios Estados miembros, o de identificar categorías de productos para las que deban organizarse acciones de control simultáneas coordinadas. En circunstancias excepcionales que requieran una intervención inmediata para preservar el buen 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.

(20) Los productos con elementos digitales deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado de productos con elementos digitales que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(21) A fin de garantizar que los fabricantes puedan publicar programas informáticos a efectos de ensayo antes de someter sus productos a la evaluación de la conformidad, los Estados miembros no deben impedir la disponibilidad de programas informáticos inacabados, como versiones *alfa*, *beta* o candidatas a la publicación, siempre y cuando la versión solo esté disponible durante el tiempo necesario para probarla y recabar información al respecto. Los fabricantes deben garantizar que los programas informáticos disponibles en estas condiciones solo se publiquen 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 que establece 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 ensayo.

(22) 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 para dichos productos. Cuando estos se modifiquen posteriormente, por medios físicos o digitales, de una manera no prevista por el fabricante y que pueda implicar que dejen de cumplir los requisitos esenciales pertinentes, dicha modificación deberá considerarse sustancial. Por ejemplo, las actualizaciones de los programas informáticos o las reparaciones pueden ser incluidas entre las operaciones de mantenimiento siempre que no modifiquen un producto ya introducido en el mercado de tal manera que puedan afectar a su observancia de los requisitos vigentes o cambiar el uso previsto para el cual se ha evaluado el producto. 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 las funciones, el tipo o las prestaciones del producto previstos originalmente y ese cambio no estuviese previsto en la evaluación inicial del riesgo; o cuando la naturaleza del peligro haya cambiado o el nivel de riesgo haya aumentado debido a la actualización de los programas informáticos.

(23) En consonancia con la noción comúnmente establecida de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, cada vez que se produzca una modificación sustancial que pueda afectar al cumplimiento del presente Reglamento por parte del producto 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 modificaciones sustanciales.

(24) La renovación, el mantenimiento y la reparación de un producto con elementos digitales, tal como se definen en el Reglamento [Reglamento sobre diseño ecológico], no conducen necesariamente a una modificación sustancial del producto, por ejemplo, si el uso previsto y las funcionalidades no se modifican y el nivel de riesgo no se ve afectado. No obstante, la mejora de un producto por parte del fabricante podría dar lugar a cambios en el diseño y el desarrollo del producto y, por tanto, podría afectar al uso previsto y a la conformidad del producto con los requisitos establecidos en el presente Reglamento.

(25) Los productos con elementos digitales deben considerarse críticos si las consecuencias negativas del aprovechamiento de posibles vulnerabilidades de ciberseguridad en el producto pueden ser graves debido a, entre otras cosas, su funcionalidad relacionada con la ciberseguridad o su uso previsto. En particular, las vulnerabilidades de los productos con elementos digitales cuya funcionalidad está relacionada con la ciberseguridad, como los elementos seguros, pueden llevar a que los problemas de seguridad se propaguen a lo largo de la cadena de suministro. La gravedad de las consecuencias de un incidente de ciberseguridad también puede acrecentarse dependiendo del uso previsto del producto, como puede ocurrir en un entorno industrial o en el contexto de una entidad esencial contemplada en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como del desempeño de funciones críticas o sensibles, como el tratamiento de datos personales.

(26) Los productos críticos con elementos digitales deben estar sujetos a procedimientos de evaluación de la conformidad más estrictos, al tiempo que se garantiza un enfoque proporcionado. A tal fin, los productos críticos con elementos digitales deben dividirse en dos clases que reflejen el nivel de riesgo de ciberseguridad presente en estas categorías de productos. Un posible incidente de ciberseguridad que afecte a productos de la clase II podría tener repercusiones negativas de mayor gravedad que un incidente que afecte a productos de la clase I, por ejemplo, debido a la naturaleza de su función vinculada a la ciberseguridad o su uso previsto en entornos sensibles, por lo que estos productos deben someterse a un procedimiento de evaluación de la conformidad más estricto.

(27) Las categorías de productos críticos con elementos digitales a que se refiere el anexo III del presente Reglamento deben entenderse como productos cuya funcionalidad principal se enumera en el anexo III del presente Reglamento. Por ejemplo, el anexo III del presente Reglamento incluye en la clase II los productos que se definen, por su funcionalidad principal, como microprocesadores de uso general. Como consecuencia de ello, los microprocesadores de uso general están sujetos a una evaluación de la conformidad por parte de terceros obligatoria. Esto no sucede con otros productos que no se mencionan explícitamente en el anexo III del presente Reglamento y que pueden llevar incorporado un microprocesador de uso general. La Comisión debe adoptar actos delegados [a más tardar doce meses después de la entrada en vigor del presente Reglamento] para especificar las definiciones de las categorías de productos comprendidas en las clases I y II, tal como se dispone en el anexo III.

(28) 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 ajenos a la ciberseguridad. Estos riesgos deben seguir

estando regulados por otra legislación pertinente de la Unión sobre productos. Si ninguna otra legislación de armonización de la Unión es aplicable, los productos deben estar sujetos al Reglamento [Reglamento relativo a la seguridad general de los productos]. 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 [Reglamento relativo a la seguridad general de los productos], el capítulo III, sección 1, los capítulos V y VII y los capítulos IX a XI del Reglamento [Reglamento relativo a la seguridad general de los productos] 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 a los efectos del [artículo 3, punto 25, del Reglamento relativo a la seguridad general de los productos].

(29) Los productos con elementos digitales considerados sistemas de inteligencia artificial (IA) de alto riesgo con arreglo al artículo 6 del Reglamento [Reglamento sobre IA][15] que entren en el ámbito de aplicación del presente Reglamento deben cumplir los requisitos esenciales establecidos en el presente Reglamento. Cuando estos sistemas de IA de alto riesgo cumplan los requisitos esenciales del presente Reglamento, debe considerarse que cumplen los requisitos de ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA] 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. 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 sujeto al presente Reglamento y considerado sistema de IA de alto riesgo, las disposiciones pertinentes del artículo 43 del Reglamento [Reglamento sobre IA] deben aplicarse como norma general en lugar de las respectivas disposiciones del presente Reglamento. Sin embargo, esta norma no debe dar lugar a una reducción del nivel de garantía necesario para los productos críticos con elementos digitales sujetos al presente Reglamento. Por consiguiente, no obstante lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA], que asimismo se consideren productos críticos con elementos digitales con arreglo al 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 [Reglamento sobre IA] deben estar sujetos a las disposiciones relativas a la evaluación de la conformidad incluidas en el presente Reglamento en la medida en que se refieran a los requisitos esenciales del presente Reglamento. En este caso, para todos los demás aspectos que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA], deben aplicarse las respectivas disposiciones relativas a la evaluación de la conformidad basadas en el control interno establecidas en el anexo VI del Reglamento [Reglamento sobre IA].

(30) Las máquinas y sus partes y accesorios que entren en el ámbito de aplicación del Reglamento [propuesta de Reglamento sobre máquinas], que sean productos con elementos digitales a los efectos del presente Reglamento y para los que se haya expedido una declaración de conformidad sobre la base del presente Reglamento deben presumirse conformes con los requisitos esenciales de salud y seguridad establecidos en el [anexo III, secciones 1.1.9 y 1.2.1] del Reglamento [propuesta de

[15] Reglamento [Reglamento sobre IA].

Reglamento sobre máquinas], en lo que respecta a la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de mando, en la medida en que la declaración UE de conformidad emitida en virtud del presente Reglamento demuestre el cumplimiento de dichos requisitos.

(31) El Reglamento [propuesta de Reglamento sobre el espacio europeo de datos sanitarios] completa los requisitos esenciales establecidos en el presente Reglamento. Por tanto, los sistemas de historiales médicos electrónicos («sistemas HME») que entren en el ámbito de aplicación del Reglamento [propuesta de Reglamento sobre el espacio europeo de datos sanitarios] y sean productos con elementos digitales a los efectos del presente Reglamento también deben cumplir los requisitos esenciales establecidos en el presente Reglamento. Sus fabricantes deben demostrar la conformidad con arreglo a lo dispuesto en el Reglamento [propuesta de Reglamento sobre el espacio europeo de datos sanitarios]. A fin de facilitar el cumplimiento, los fabricantes pueden elaborar una única documentación técnica que contenga los elementos requeridos por ambos actos jurídicos. Dado que el presente Reglamento no regula el SaaS propiamente dicho, los sistemas HME que se ofrezcan a través del modelo de concesión de licencias y distribución del SaaS no entran en el ámbito de aplicación del presente Reglamento. Del mismo modo, los sistemas HME desarrollados y utilizados internamente no entran en el ámbito de aplicación del presente Reglamento, ya que no se introducen en el mercado.

(32) Para garantizar que los productos con elementos digitales sean seguros tanto en el momento de su introducción en el mercado como a lo largo de su ciclo de vida, es necesario establecer requisitos esenciales para la gestión de las vulnerabilidades y requisitos esenciales de ciberseguridad relativos a las propiedades de los productos con elementos digitales. Si bien los fabricantes deben cumplir todos los requisitos esenciales en relación con la gestión de las vulnerabilidades y garantizar que todos sus productos se entreguen sin ninguna vulnerabilidad aprovechable conocida, también deben determinar qué otros requisitos esenciales relacionados con las propiedades del producto son pertinentes para el tipo de producto 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 pertinentes y aplicar adecuadamente las normas armonizadas o especificaciones comunes apropiadas.

(33) Para mejorar la seguridad de los productos con elementos digitales comercializados en el mercado interior, es necesario establecer requisitos esenciales. Dichos requisitos deben entenderse sin perjuicio de las evaluaciones coordinadas de riesgos de la UE que se efectúen con respecto a las cadenas de suministro críticas, según lo establecido en el [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)][16], 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, en la evaluación coordinada de riesgos 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

[16] Directiva XXX del Parlamento Europeo y del Consejo, de [fecha], [relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión y por la que se deroga la Directiva (UE) 2016/1148 (DO L xx de fecha, p. x)].

5G acordado por el Grupo de Cooperación SRI a que hace referencia la [Directiva XXX/XXXX (SRI 2)].

(34) Para garantizar que los CSIRT nacionales y los puntos de contacto únicos designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XX/XXXX (SRI 2)] reciban la información necesaria para desempeñar sus funciones y aumentar el nivel general de ciberseguridad de las entidades esenciales e importantes, así como para garantizar el funcionamiento efectivo de las autoridades de vigilancia del mercado, los fabricantes de productos con elementos digitales deben notificar a la ENISA las vulnerabilidades que se estén aprovechando activamente. 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. Los fabricantes también deben considerar la posibilidad de divulgar las vulnerabilidades subsanadas en la base de datos europea de vulnerabilidades creada en virtud de la Directiva [Directiva XX/XXXX (SRI 2)] y gestionada por la ENISA o en cualquier otra base de datos de vulnerabilidades que sea de acceso público.

(35) Los fabricantes también deben notificar a la ENISA cualquier incidente que repercuta en la seguridad del producto con elementos digitales. Sin perjuicio de las obligaciones de notificación de incidentes establecidas en la Directiva [Directiva XXX/XXXX (SRI 2)] para las entidades esenciales e importantes, es fundamental que los fabricantes de productos con elementos digitales proporcionen a la ENISA, a los puntos de contacto únicos designados por los Estados miembros de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] y a las autoridades de vigilancia del mercado información que les permita evaluar la seguridad de dichos productos. Para garantizar que los usuarios puedan reaccionar rápidamente ante incidentes 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 mitigar 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 lo justifiquen, comunicándose directamente con ellos.

(36) 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. Una política de divulgación coordinada de vulnerabilidades 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. 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 (los denominados «programas de recompensa por detección de errores» o «bug bounty»).

(37) A fin de facilitar el análisis de las vulnerabilidades, los fabricantes deben especificar y documentar los componentes contenidos en los productos con elementos digitales, en particular mediante la elaboración de una nomenclatura de materiales de los programas

informáticos. Una nomenclatura de materiales de los programas informáticos 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, sobre todo ayudar a los fabricantes y a los usuarios a rastrear las vulnerabilidades y los riesgos conocidos de reciente aparición. Es de particular importancia que los fabricantes garanticen que sus productos no contengan componentes vulnerables desarrollados por terceros.

(38) 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 del presente Reglamento en especificaciones técnicas detalladas y se adopten con arreglo al Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[17]. El Reglamento (UE) n.º 1025/2012 establece un procedimiento de presentación de objeciones a las normas armonizadas para el caso en que estas no cumplan plenamente los requisitos del presente Reglamento.

(39) 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 aplicarse a productos con elementos digitales regulados por el presente Reglamento. El presente Reglamento debe crear 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 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 del presente Reglamento en la medida en que el certificado 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. Estos futuros esquemas europeos de certificación de la ciberseguridad que se apliquen a productos con elementos digitales deben tener en cuenta los requisitos esenciales establecidos en el presente Reglamento y facilitar su cumplimiento. La Comisión debe estar facultada para especificar, mediante actos de ejecución, los esquemas europeos de certificación de la ciberseguridad que puedan utilizarse para demostrar la conformidad con los requisitos esenciales establecidos en el presente Reglamento. Además, con el fin de evitar cargas administrativas excesivas para los fabricantes, la Comisión debe, cuando proceda, especificar si un certificado de ciberseguridad expedido en el marco de dichos esquemas europeos de certificación de la ciberseguridad elimina la obligación 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.

---

[17] 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).

(40) Tras la entrada en vigor del acto de ejecución por el que se establece el [Reglamento de Ejecución (UE) n.º .../... de la Comisión, de XXX, relativo al esquema europeo de certificación de la ciberseguridad basado en criterios comunes], que regula los productos consistentes en equipos informáticos sujetos al presente Reglamento, como los módulos de seguridad y los microprocesadores de los equipos informáticos, la Comisión podrá especificar, mediante acto de ejecución, el modo en que el esquema europeo de certificación de la ciberseguridad supone la presunción de conformidad con los requisitos esenciales especificados en el anexo I del presente Reglamento o partes de estos. Además, dicho acto de ejecución podrá especificar la medida en que un certificado expedido en virtud del 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.

(41) Cuando no se adopten normas armonizadas o cuando las normas armonizadas no tengan suficientemente en cuenta los requisitos esenciales del presente Reglamento, la Comisión debe poder adoptar especificaciones comunes mediante actos de ejecución. Las razones para elaborar estas especificaciones comunes en lugar de basarse en normas armonizadas pueden incluir la denegación de la solicitud de normalización por parte de cualquiera de los organismos europeos de normalización, retrasos indebidos en el establecimiento de normas armonizadas apropiadas o la falta de conformidad de las normas establecidas con los requisitos del presente Reglamento o con una petición de la Comisión. Para facilitar la evaluación de la conformidad con los requisitos esenciales 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.

(42) 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 del presente Reglamento y, cuando proceda, de otra legislación de armonización de la Unión aplicable al producto. También puede obligarse a los fabricantes a preparar una declaración UE de conformidad con arreglo a otras normas de la Unión. Para garantizar un acceso efectivo a la información con fines de vigilancia del mercado, deberá prepararse una única declaración UE de conformidad relativa al cumplimiento de todos los actos 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.

(43) 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[18]. 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

[18] 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).

que garantice que los productos con elementos digitales cumplen con los requisitos del presente Reglamento.

(44) Para que los operadores económicos puedan demostrar la conformidad con los requisitos esenciales 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[19] 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 establecidos en el presente Reglamento se han basado 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, en particular la planificación, el diseño, el desarrollo o la producción, los ensayos y el mantenimiento del producto.

(45) Como norma general, el fabricante debe llevar a cabo la evaluación de la conformidad de los productos con elementos digitales bajo su propia responsabilidad mediante un procedimiento basado en el módulo A de la Decisión n.º 768/2008/CE. El fabricante deberá ser flexible en lo que se refiere a la elección de un procedimiento de evaluación de la conformidad más estricto en el que participe un tercero. Si el producto está considerado producto crítico de la clase I, se requieren garantías adicionales para demostrar la conformidad con los requisitos esenciales 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 de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 que hayan sido reconocidos por la Comisión mediante acto de ejecución. Si el fabricante no aplica estas normas armonizadas, especificaciones comunes o esquemas de certificación de la ciberseguridad, debe someterse a una evaluación de la conformidad en la que participe un tercero. 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 + 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 críticos con los elementos digitales de manera proporcionada y eficaz. El fabricante que opte por la evaluación de la conformidad de terceros puede elegir el procedimiento que mejor se adapte a su proceso de diseño y producción. Habida cuenta del riesgo de ciberseguridad aún mayor asociado al uso de productos clasificados como productos críticos de la clase II, la evaluación de la conformidad de estos productos siempre debe contar con la participación de un tercero.

(46) 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

[19] 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).

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 del presente Reglamento a lo largo de las fases de diseño, desarrollo y producción.

(47) 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, fundamentalmente en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses.

(48) 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.

(49) 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.

(50) 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.

(51) 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). 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.

(52) 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.

(53) En interés 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 estos 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.

(54) La vigilancia del mercado es un instrumento esencial para garantizar la aplicación correcta y uniforme de la legislación 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 del Parlamento Europeo y del Consejo[20] se aplican a los productos con elementos digitales regulados por el presente Reglamento.

(55) De conformidad con el Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado son responsables de efectuar la vigilancia del mercado en el territorio del Estado miembro correspondiente. El presente Reglamento no debe impedir que los Estados miembros escojan a las autoridades competentes que desempeñan esas tareas. Cada Estado miembro debe designar a una o varias autoridades de vigilancia del mercado en su territorio. Los Estados miembros podrán 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 especificadas en el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] y las autoridades nacionales de certificación de la ciberseguridad designadas a las que hace referencia el artículo 58 del Reglamento (UE) 2019/881. 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 relacionadas con el presente Reglamento. De conformidad con el 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.

(56) Debe establecerse un Grupo de Cooperación Administrativa (ADCO) específico para la aplicación uniforme del presente Reglamento, de conformidad con el artículo 30,

[20] 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).

apartado 2, del Reglamento (UE) 2019/1020. Este 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 sobre la base 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, sus subgrupos y este ADCO. También debe ayudar a este ADCO por medio de una secretaría ejecutiva que preste apoyo técnico y logístico.

(57) 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 en virtud del 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.

(58) 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 de información electrónico por entidades esenciales contempladas en el [anexo I de la Directiva XXX/XXXX (SRI 2)] o para otros aspectos relativos a la protección del interés público. Es por tanto necesario establecer normas que garanticen la mitigación 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 presente dicho riesgo, retirarlo del mercado o recuperarlo, dependiendo del riesgo que presente. Tan pronto como una autoridad de vigilancia del mercado restrinja o prohíba la libre circulación de un producto 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 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 puede considerar la adopción de propuestas para revisar la legislación de la Unión que corresponda.

(59) 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 no son conformes con el presente Reglamento, o bien a los productos que son conformes con el presente Reglamento pero presentan otros riesgos importantes, como riesgos para la salud o la seguridad de las personas, los derechos fundamentales o la prestación de servicios por parte de entidades esenciales del tipo contemplado en el [anexo I de la Directiva XXX/XXXX (SRI 2)], la Comisión podrá solicitar a la ENISA que lleve a cabo una evaluación. Sobre la base de dicha evaluación, la Comisión podrá adoptar, mediante actos de ejecución, medidas correctoras o restrictivas a escala de la Unión, como retirar del mercado o recuperar los productos correspondientes en un plazo razonable, proporcional a la naturaleza del riesgo. La Comisión solo puede recurrir a tal medida en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y únicamente cuando las autoridades de vigilancia no hayan adoptado medidas eficaces para remediar la situación. Estas 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 no conforme utilizado asimismo en sectores clave por entidades incluidas en el ámbito de aplicación de la [Directiva XXX/XXXX (SRI 2)], 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 podrá 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.

(60) En los casos en que 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.

(61) 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 presentan a menudo riesgos de ciberseguridad graves. La ENISA debe presentar a las autoridades de vigilancia del mercado propuestas de categorías de productos para las que podrían organizarse barridos, sobre la base, entre otras cosas, de las notificaciones que reciba relativas a vulnerabilidades e incidentes de los productos.

(62) 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 a efectos de actualizar la lista de productos críticos del anexo III y especificar las definiciones de dichas categorías de productos. 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 alcancen el mismo nivel de protección que el presente Reglamento, especificando 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 de determinados productos altamente críticos con elementos digitales, sobre la base de

criterios de criticidad establecidos en el presente Reglamento, así como con respecto a la especificación del contenido mínimo de la declaración UE de conformidad y al complemento de los elementos que deban incluirse en la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional sobre la Mejora de la Legislación, de 13 de abril de 2016[21]. 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.

(63) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para: especificar el formato y los elementos de la nomenclatura de materiales de los programas informáticos; especificar el tipo de información, el formato y el procedimiento para las notificaciones de vulnerabilidades aprovechadas activamente e incidentes presentadas por los fabricantes a la ENISA; especificar los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que puedan utilizarse para demostrar la conformidad con los requisitos esenciales, o partes de estos, establecidos en el anexo I del presente Reglamento; adoptar especificaciones comunes relacionadas con los requisitos esenciales establecidos en el anexo I; establecer especificaciones técnicas para los pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales y mecanismos para promover su uso; y adoptar decisiones sobre medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[22].

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

(65) 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, en particular si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por infracciones similares.

---

21 DO L 123 de 12.5.2016, p. 1.

22 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).

Tales circunstancias pueden ser agravantes, en situaciones en las que la infracción cometida por el mismo operador persista en el territorio de Estados miembros distintos de aquel en el que ya se haya impuesto una multa administrativa, o bien atenuantes, si se garantiza 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, una sanción impuesta en otros Estados miembros y la cuantía de esta. En todos estos casos, la multa administrativa acumulada que podrían 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.

(66) Si las multas administrativas se imponen a personas que no son 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.

(67) En sus relaciones con terceros países, la UE 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 certificados, marcas de conformidad e informes de ensayos emitidos por los organismos de evaluación de la conformidad de cualquiera de las partes de conformidad con la legislación de la otra parte. Actualmente hay ARM vigentes con varios países. Se han celebrado acuerdos de este tipo en varios sectores específicos que pueden variar entre 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 Tratado de Funcionamiento de la Unión Europea (TFUE), puede celebrar ARM relativos a la evaluación de la conformidad de los productos regulados por el presente Reglamento. La cooperación con los países socios 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 UE.

(68) La Comisión debe revisar periódicamente lo dispuesto en el presente Reglamento, en consulta con las partes interesadas, en particular para determinar si se precisa alguna modificación a raíz de cambios en la situación social, política, tecnológica o del mercado.

(69) Los operadores económicos deben disponer de tiempo suficiente para adaptarse a los requisitos del presente Reglamento. El presente Reglamento debe ser aplicable [veinticuatro meses] después de su entrada en vigor, a excepción de las obligaciones de información relativas a vulnerabilidades aprovechadas activamente e incidentes, que deben ser aplicables [doce meses] después de la entrada en vigor del presente Reglamento.

(70) 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 nivel de la Unión, la Unión puede adoptar medidas, de acuerdo con el

principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De acuerdo con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(71) 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[23], emitió su dictamen el […],

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

El presente Reglamento establece:

a) normas para la introducción en el mercado de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos;

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

c) requisitos esenciales para los procesos de gestión de la vulnerabilidad establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales a lo largo de todo el ciclo de vida, y las obligaciones de los operadores económicos en relación con dichos procesos;

d) normas relativas a la vigilancia del mercado y a la aplicación de los requisitos y las normas antes mencionados.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento es aplicable a los productos con elementos digitales cuyo uso previsto o 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 de la Unión:

   a) el Reglamento (UE) 2017/745;

   b) el Reglamento (UE) 2017/746;

[23] 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).

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. 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 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 alcancen un nivel de protección equivalente al previsto en el presente Reglamento.

La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de modificar el presente Reglamento, especificando si dicha limitación o exclusión es necesaria, los productos y normas afectados y, si procede, el alcance de la limitación.

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

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

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

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

3) «producto crítico con elementos digitales»: un producto con elementos digitales que presenta un riesgo de ciberseguridad de conformidad con los criterios establecidos en el artículo 6, apartado 2, y cuya función principal se establece en el anexo III;

4) «producto altamente crítico con elementos digitales»: un producto con elementos digitales que presenta un riesgo de ciberseguridad de conformidad con los criterios establecidos en el artículo 6, apartado 5;

5) «tecnología operativa»: sistemas o dispositivos digitales programables que interactúan con el entorno físico o administran dispositivos que interactúan con el entorno físico;

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

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

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

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

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

11) «conexión física»: cualquier conexión entre sistemas de información o componentes electrónicos ejecutada por medios físicos, incluso a través de interfaces eléctricas o mecánicas, cables u ondas de radio;

12) «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;

13) «privilegio»: un derecho de acceso concedido a usuarios o programas concretos para llevar a cabo operaciones pertinentes en materia de seguridad dentro de un sistema electrónico de información;

14) «privilegio elevado»: un derecho de acceso concedido a usuarios o programas concretos para llevar a cabo un conjunto ampliado de operaciones pertinentes en materia de seguridad dentro de un sistema electrónico de información, que, si se utiliza indebidamente o se ve comprometido, podría permitir a un agente malintencionado obtener un mayor acceso a los recursos de un sistema u organización;

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

16) «recursos de red o informáticos»: funcionalidad de datos o de equipos o programas informáticos accesible a nivel local o a través de una red o de otro dispositivo conectado;

17) «operador económico»: el fabricante, el representante autorizado, el importador, el distribuidor o cualquier otra persona física o jurídica sujeta a las obligaciones establecidas en el presente Reglamento;

18) «fabricante»: toda 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 o gratuita;

19) «representante autorizado»: toda persona física o jurídica establecida en la Unión que ha recibido un mandato escrito de un fabricante para actuar en su nombre en relación con tareas especificadas;

20) «importador»: toda 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;

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

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

23) «comercialización»: todo 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;

24) «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;

25) «uso razonablemente previsible»: uso que no corresponde necesariamente a 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;

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

27) «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;

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

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

30) «organismo notificado»: un organismo de evaluación de la conformidad designado con arreglo al artículo 33 del presente Reglamento y otras normas de armonización pertinentes de la Unión;

31) «modificación sustancial»: un cambio en un producto con elementos digitales tras su introducción en el mercado que afecta al cumplimiento por parte del producto de los requisitos esenciales establecidos en la sección 1 del anexo I o que provoca la modificación de la finalidad prevista para la que se ha evaluado el producto con elementos digitales;

32) «marcado CE»: un 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 establecidos en el anexo I y otras normas de la Unión aplicables que armonicen las condiciones para la comercialización de productos (las «normas de armonización de la Unión») y prevean su colocación;

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

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

35) «riesgo de ciberseguridad»: un riesgo tal como se define en el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)];

36) «riesgo de ciberseguridad significativo»: un 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, en particular causando pérdidas o perturbaciones materiales o inmateriales considerables;

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

38) «vulnerabilidad»: una vulnerabilidad tal como se define en el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)];

39) «vulnerabilidad aprovechada activamente»: una vulnerabilidad respecto de la cual existen pruebas fiables de la ejecución de un código malicioso en un sistema por parte de un agente sin autorización del propietario del sistema;

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

Artículo 4

Libre circulación

1. Los Estados miembros no impedirán, por los aspectos contemplados 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 y usen productos con elementos digitales que no sean conformes con el presente Reglamento.

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 a efectos de ensayo, y que se indique con claridad, mediante una señal visible, que no son conformes con el presente Reglamento y que no se comercializarán con fines distintos de su ensayo.

Artículo 5

Requisitos aplicables a los productos con elementos digitales

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

1) cumplen los requisitos esenciales establecidos en la sección 1 del anexo I, a condición de que hayan sido instalados de manera adecuada, mantenidos y utilizados para los fines previstos o en condiciones que se puedan prever razonablemente y, en su caso, actualizados, y si

2) los procesos establecidos por el fabricante cumplen los requisitos esenciales establecidos en la sección 2 del anexo I.

Artículo 6

Productos críticos con elementos digitales

1. Los productos con elementos digitales que pertenezcan a una categoría mencionada en el anexo III se considerarán productos críticos con elementos digitales. Los productos que tengan una función principal de una categoría mencionada en el

anexo III del presente Reglamento se considerarán incluidos en dicha categoría. Las categorías de productos críticos con elementos digitales se dividirán en las clases I y II, tal como se establece en el anexo III, para reflejar el nivel de riesgo de ciberseguridad asociado a dichos productos.

2. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de modificar el anexo III para incluir una nueva categoría en la lista de categorías de productos críticos con elementos digitales o retirar una categoría de dicha lista. A la hora de evaluar la necesidad de modificar la lista del anexo III, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad asociado a la categoría de productos con elementos digitales. Para determinar el nivel de riesgo de ciberseguridad, se tendrán en cuenta uno o varios de los criterios siguientes:

   a) la funcionalidad relacionada con la ciberseguridad del producto con elementos digitales y si el producto con elementos digitales tiene al menos uno de los siguientes atributos:

      i) está diseñado para funcionar con un privilegio elevado o para gestionar privilegios;

      ii) tiene acceso directo o privilegiado a redes o recursos informáticos;

      iii) está diseñado para controlar el acceso a datos o a tecnología operativa;

      iv) desempeña una función esencial para la confianza, en particular funciones de seguridad como el control de las redes, la seguridad de los nodos finales y la protección de las redes;

   b) el uso previsto en entornos sensibles, en particular en entornos industriales o por parte de entidades esenciales contempladas en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)];

   c) el uso previsto relativo a la realización de funciones críticas o sensibles, como el tratamiento de datos personales;

   d) el posible alcance potencial de las repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a una pluralidad de personas;

   e) la medida en que el uso de productos con elementos digitales ya ha causado pérdidas o perturbaciones materiales o inmateriales o ha dado lugar a preocupaciones importantes en relación con la materialización de repercusiones negativas.

3. La Comisión estará facultada para adoptar un acto delegado con arreglo al artículo 50 a fin de completar el presente Reglamento mediante la especificación de las definiciones de las categorías de productos de las clases I y II que figuran en el anexo III. El acto delegado se adoptará [a más tardar doce meses después de la entrada en vigor del presente Reglamento].

4. Los productos críticos con elementos digitales estarán sujetos a los procedimientos de evaluación de la conformidad especificados en el artículo 24, apartados 2 y 3.

5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 50 a fin de completar el presente Reglamento mediante el establecimiento de categorías de productos altamente críticos con elementos digitales, cuyos fabricantes deberán obtener un certificado europeo de ciberseguridad expedido en el marco de un esquema europeo de certificación de la ciberseguridad con arreglo al Reglamento

(UE) 2019/881 con el fin de demostrar la conformidad con los requisitos esenciales establecidos en el anexo I o parte de ellos. A la hora de determinar dichas categorías de productos altamente críticos con elementos digitales, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad asociado a la categoría de productos con elementos digitales, a la luz de uno o varios de los criterios enumerados en el apartado 2 y de la evaluación que determine si dicha categoría de productos:

a) es utilizada por las entidades esenciales del tipo contemplado en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)], si sirve a estas de referencia o si, en el futuro, podría desempeñar un papel importante para las actividades de estas entidades; o

b) si resulta pertinente para la resiliencia la cadena de suministro global de productos con elementos digitales frente a las perturbaciones.

Artículo 7

Seguridad general de los productos

No obstante lo dispuesto en el artículo 2, apartado 1, párrafo tercero, letra b), del Reglamento [Reglamento relativo a la seguridad general de los productos], cuando los productos con elementos digitales no estén sujetos a requisitos específicos establecidos en otras normas de armonización de la Unión en el sentido del [artículo 3, punto 25, del Reglamento relativo a la seguridad general de los productos], el capítulo III, sección 1, los capítulos V y VII, y los capítulos IX a XI del Reglamento [Reglamento relativo a la seguridad general de los productos] serán aplicables a dichos productos en lo que respecta a los riesgos para la seguridad no contemplados en el presente Reglamento.

Artículo 8

Sistemas de IA de alto riesgo

1. Los productos con elementos digitales clasificados como sistemas de IA de alto riesgo de conformidad con el artículo [artículo 6] del Reglamento [Reglamento sobre IA] que entran en el ámbito de aplicación del presente Reglamento y cumplen los requisitos esenciales establecidos en la sección 1 del anexo I del presente Reglamento, siempre que los procesos establecidos por el fabricante cumplan los requisitos esenciales establecidos en la sección 2 del anexo I, se considerarán conformes con los requisitos relativos a la ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA], sin perjuicio de los demás requisitos relativos a la precisión y la solidez incluidos en el citado artículo, en la medida en que la consecución del nivel de protección exigido por dichos requisitos se demuestre mediante la declaración UE de conformidad expedida en virtud del presente Reglamento.

2. Para los productos y los requisitos de ciberseguridad mencionados en el apartado 1, será aplicable el procedimiento de evaluación de la conformidad pertinente de conformidad con el artículo [artículo 43] del Reglamento [Reglamento sobre IA]. A efectos de dicha evaluación, los organismos notificados que dispongan de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA] también dispondrán de la facultad de 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 su anexo I, a condición de que se haya evaluado el cumplimiento por parte de dichos

organismos notificados de los requisitos dispuestos en el artículo 29 del presente Reglamento en el contexto del procedimiento de notificación contemplado en el Reglamento [Reglamento sobre IA].

3. No obstante lo dispuesto en el apartado 2, los productos críticos con elementos digitales enumerados en el anexo III del presente Reglamento que requieran la aplicación de los procedimientos de evaluación de la conformidad establecidos en el artículo 24, apartado 2, letras a) y b), y el artículo 24, apartado 3, letras a) y b), del presente Reglamento, que también estén clasificados como sistemas de IA de alto riesgo con arreglo al artículo [artículo 6] del Reglamento [Reglamento sobre IA] y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo [anexo VI] del Reglamento [Reglamento sobre IA] estarán sujetos a los procedimientos de evaluación de la conformidad exigidos por el presente Reglamento en lo que respecta a los requisitos esenciales del presente Reglamento.

Artículo 9

Máquinas y sus partes y accesorios

Las máquinas y sus partes y accesorios que entren en el ámbito de aplicación del Reglamento [propuesta de Reglamento sobre máquinas], que sean productos con elementos digitales en el sentido del presente Reglamento y para los que se haya expedido una declaración UE de conformidad sobre la base del presente Reglamento se presumirán conformes con los requisitos esenciales de salud y seguridad establecidos en el anexo [anexo III, secciones 1.1.9 y 1.2.1] del Reglamento [propuesta de Reglamento sobre máquinas], en lo que respecta a la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de mando, en la medida en que la declaración UE de conformidad emitida en virtud del presente Reglamento demuestre el cumplimiento del nivel de protección exigido por dichos requisitos.

CAPÍTULO II

OBLIGACIONES DE LOS OPERADORES ECONÓMICOS

Artículo 10

Obligaciones de los fabricantes

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

2. A efectos del cumplimiento de la obligación establecida en el 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 de seguridad y reducir al mínimo las repercusiones de dichos incidentes, incluidas las relacionadas con la salud y la seguridad de los usuarios.

3. Al introducir en el mercado un producto con elementos digitales, el fabricante incluirá en la documentación técnica una evaluación de riesgos de ciberseguridad, tal

como se establece en el artículo 23 y en el anexo V. En el caso de los productos con elementos digitales a que se refieren el artículo 8 y el artículo 24, apartado 4, que también estén sujetos a otros actos de la Unión, la evaluación de los riesgos de ciberseguridad podrá formar parte de la evaluación de riesgos exigida por los actos de la Unión que correspondan. Cuando determinados requisitos esenciales no sean aplicables al producto con elementos digitales comercializado, el fabricante incluirá una justificación clara en dicha documentación.

4. A efectos del cumplimiento de la obligación establecida en el apartado 1, los fabricantes ejercerán la diligencia debida al integrar componentes procedentes de terceros en productos con elementos digitales. Velarán por que dichos componentes no comprometan la seguridad del producto con elementos digitales.

5. El fabricante documentará 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, actualizará la evaluación de riesgos del producto.

6. Desde la introducción de un producto con elementos digitales en el mercado y durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto en el mercado, si este período fuese más breve, los fabricantes velarán por que las vulnerabilidades de dicho producto se gestionen de manera eficaz y de conformidad con los requisitos esenciales establecidos en la sección 2 del anexo I.

   Los fabricantes contarán con políticas y procedimientos adecuados, incluidas las políticas de divulgación coordinada de vulnerabilidades a que se refiere la sección 2, punto 5, del anexo I, para tratar y subsanar las posibles vulnerabilidades del producto con elementos digitales comunicadas por fuentes internas o externas.

7. Antes de introducir en el mercado un producto con elementos digitales, los fabricantes elaborarán la documentación técnica especificada en el artículo 23.

   También aplicarán o mandarán aplicar los procedimientos de evaluación de la conformidad de su elección a que se hace referencia en el artículo 24.

   Cuando mediante dicho procedimiento de evaluación de la conformidad se haya demostrado la conformidad del producto con elementos digitales con los requisitos esenciales establecidos en la sección 1 del anexo I y la conformidad de los procesos establecidos por el fabricante con los requisitos esenciales establecidos en la sección 2 del anexo I, los fabricantes elaborarán la declaración UE de conformidad con arreglo al artículo 20 y colocarán el marcado CE con arreglo al artículo 22.

8. Los fabricantes mantendrán la documentación técnica y la declaración UE de conformidad, cuando proceda, a disposición de las autoridades de vigilancia del mercado durante diez años a partir de la introducción en el mercado del producto con elementos digitales.

9. 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. El fabricante tomará 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 hace referencia en el artículo 19 en virtud de las cuales se declara o por aplicación de las cuales se verifica la conformidad del producto.

10. Los fabricantes se asegurarán de que los productos con elementos digitales vayan acompañados de la información y las instrucciones especificadas en el anexo II, en formato electrónico o físico. Dichas instrucciones e información figurarán en una lengua fácilmente comprensible para los usuarios. Serán claras, comprensibles, inteligibles y legibles. Permitirán la instalación, el funcionamiento y el uso seguros de los productos con elementos digitales.

11. Los fabricantes entregarán la declaración UE de conformidad junto con el producto con elementos digitales o incluirán en las instrucciones y la información especificadas en el anexo II la dirección de internet donde se pueda acceder a la declaración UE de conformidad.

12. Desde la introducción en el mercado de un producto con elementos digitales y durante la vida útil prevista del producto o durante cinco años a partir de la introducción en el mercado del producto, si este período fuese más breve, 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 establecidos en el anexo I adoptarán inmediatamente las medidas correctoras necesarias para que el producto con elementos digitales o los procesos del fabricante sean conformes, para retirarlo del mercado o para recuperarlo, según proceda.

13. 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 establecidos en el anexo I. 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.

14. El fabricante que cese sus actividades y, en consecuencia, no pueda cumplir las obligaciones establecidas en el presente Reglamento informará de esta situación, 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 productos con elementos digitales introducidos en el mercado que se vean afectados.

15. La Comisión podrá especificar, mediante actos de ejecución, el formato y los elementos de la nomenclatura de materiales de los programas informáticos establecida en la sección 2, punto 1, del anexo I. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 51, apartado 2.

Artículo 11

Obligaciones de información de los fabricantes

1. El fabricante notificará a la ENISA, sin demora indebida, y en cualquier caso en un plazo de veinticuatro horas a partir del momento en que tenga conocimiento de ello, cualquier vulnerabilidad aprovechada activamente presente en el producto con

elementos digitales. La notificación incluirá información detallada sobre dicha vulnerabilidad y, en su caso, sobre las medidas correctoras o paliativas adoptadas. La ENISA transmitirá la notificación tras su recepción, sin demora indebida salvo por motivos justificados en relación con los riesgos de ciberseguridad, al CSIRT designado a efectos de la divulgación coordinada de vulnerabilidades con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará a la autoridad de vigilancia del mercado sobre la vulnerabilidad notificada.

2. El fabricante notificará a la ENISA, sin demora indebida, y en cualquier caso en un plazo de veinticuatro horas a partir del momento en que tenga conocimiento de ello, cualquier incidente que afecte al producto con elementos digitales. La ENISA transmitirá la notificación, sin demora indebida, salvo por motivos justificados en relación con los riesgos de ciberseguridad, al punto único de contacto designado con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará a la autoridad de vigilancia del mercado sobre los incidentes notificados. La notificación del incidente incluirá información sobre la gravedad y las repercusiones del incidente y, en su caso, indicará si el fabricante sospecha que el incidente ha sido causado por actos ilícitos o malintencionados o si considera que tiene repercusiones transfronterizas.

3. La ENISA presentará a la red de organizaciones de enlace para la gestión de cibercrisis de la UE (CyCLONe) creada por el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] la información notificada con arreglo a los apartados 1 y 2 si dicha información es pertinente para la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo.

4. El fabricante informará, sin demora indebida y una vez tenga conocimiento de ello, a los usuarios del producto con elementos digitales sobre el incidente y, cuando así se requiera, sobre las medidas correctoras que el usuario pueda adoptar para mitigar las repercusiones del incidente.

5. La Comisión podrá, mediante actos de ejecución, especificar el tipo de información, el formato y el procedimiento de las notificaciones presentadas con arreglo a los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.

6. Sobre la base de las notificaciones recibidas con arreglo a los apartados 1 y 2, la ENISA elaborará un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en los productos con elementos digitales y lo presentará al Grupo de Cooperación especificado en el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)]. 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 los apartados 1 y 2.

7. Al detectar una vulnerabilidad en un componente, incluso si este es de código abierto, integrado en el producto con elementos digitales, los fabricantes notificarán la vulnerabilidad a la persona o entidad a cargo del mantenimiento del componente.

Artículo 12

Representantes autorizados

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

2. Las obligaciones establecidas en el artículo 10, apartados 1 a 7, primer guion, y 9, no formarán parte del mandato del representante autorizado.

3. El representante autorizado efectuará las tareas especificadas en el mandato recibido del fabricante. 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 20 y la documentación técnica a que se refiere el artículo 23 a disposición de las autoridades de vigilancia del mercado durante diez años a partir de la introducción en el mercado del producto con elementos digitales;

   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 que presente un producto con elementos digitales objeto del mandato del representante autorizado.

Artículo 13

Obligaciones de los importadores

1. Los importadores solo introducirán en el mercado productos con elementos digitales que cumplan los requisitos esenciales establecidos en la sección 1 del anexo I, y siempre que los procesos establecidos por el fabricante cumplan los requisitos esenciales establecidos en la sección 2 del anexo I.

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 los que hace referencia el artículo 24;

   b) el fabricante ha redactado la documentación técnica;

   c) el producto con elementos digitales lleva el marcado CE contemplado en el artículo 22 y va acompañado de la información y las instrucciones de uso especificadas en el anexo II.

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 los requisitos esenciales establecidos en el anexo I, no lo introducirá en el mercado hasta que el producto o los procesos establecidos por el fabricante no se hayan llevado a la conformidad con los requisitos esenciales establecidos en el anexo I. 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.

4. Los importadores indicarán su nombre, nombre comercial registrado o marca registrada, su dirección postal y su dirección de correo electrónico de contacto en el producto con elementos digitales o, cuando no sea posible, 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 garantizarán que el producto con elementos digitales vaya acompañado de las instrucciones y la información establecidas en el anexo II, en una lengua fácilmente comprensible para los usuarios.

6. Los importadores que sepan o tengan motivos para creer que un producto con elementos digitales que han introducido en el mercado o los procesos establecidos por su fabricante no son conformes con los requisitos esenciales establecidos en el anexo I adoptarán inmediatamente las medidas correctoras necesarias para que dicho producto con elementos digitales o los procesos establecidos por su fabricante sean conformes con los requisitos esenciales establecidos en el anexo I, o bien para retirarlo del mercado o recuperarlo, cuando proceda.

   Al detectar 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 comercializaron y proporcionarán detalles, en particular, sobre la no conformidad y cualquier medida correctora adoptada.

7. Durante un período de diez años a partir de la introducción del producto con elementos digitales en el mercado, los importadores mantendrán 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.

8. 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 establecidos en la sección 1 del anexo I, así como la conformidad de los procesos establecidos por el fabricante con los requisitos esenciales establecidos en el sección 2 del anexo I. 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.

9. Cuando el importador de un producto con elementos digitales tenga conocimiento de que el fabricante haya cesado sus actividades y, en consecuencia, no pueda 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 productos con elementos digitales introducidos en el mercado que se vean afectados.

Artículo 14

Obligaciones de los distribuidores

1. Al comercializar un producto con elementos digitales, los distribuidores actuarán con la diligencia debida en relación con los requisitos del 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 10, apartados 10 y 11, y en el artículo 13, apartado 4.

3. Si un distribuidor considera o tiene motivos para creer que un producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales 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 llevado a conformidad. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, el distribuidor informará de ello al fabricante y a las autoridades de vigilancia del mercado.

4. Los distribuidores que sepan o tengan motivos para creer que un producto con elementos digitales que han comercializado o los procesos establecidos por su fabricante no son conformes con los requisitos esenciales establecidos en el anexo I se asegurarán de que se adopten las medidas correctoras necesarias para que dicho producto con elementos digitales o los procesos establecidos por su fabricante sean conformes con dichos requisitos, o bien para retirarlo del mercado o recuperarlo, cuando proceda.

   Al detectar 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 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 los requisitos esenciales establecidos en el anexo I. 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 han comercializado.

6. Cuando el distribuidor de un producto con elementos digitales tenga conocimiento de que el fabricante haya cesado sus actividades y, en consecuencia, no pueda cumplir las obligaciones establecidas en el presente Reglamento, el distribuidor 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 productos con elementos digitales introducidos en el mercado que se vean afectados.

Artículo 15

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, que, por consiguiente, estará sujeto a las obligaciones del fabricante establecidas en el artículo 10 y en el artículo 11, apartados 1, 2, 4 y 7, 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 16

Otros casos en que son aplicables las obligaciones de los fabricantes

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 del producto con elementos digitales.

Esta persona estará sujeta a las obligaciones del fabricante establecidas en el artículo 10 y en el artículo 11, apartados 1, 2, 4 y 7, con respecto a la parte del producto 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 17

Identificación de los operadores económicos

1. Los operadores económicos facilitarán, previa solicitud y cuando se disponga de la información, 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) el nombre y la dirección de cualquier operador económico al que hayan suministrado un producto con elementos digitales.

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

CAPÍTULO III

CONFORMIDAD DEL PRODUCTO CON ELEMENTOS DIGITALES

Artículo 18

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 salud y seguridad establecidos en el anexo I que estén regulados por dichas normas o partes de ellas.

2. Se presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante que sean conformes con las especificaciones comunes a que hace referencia el artículo 19 son conformes con los requisitos esenciales establecidos en el anexo I, en la medida en que dichas especificaciones comunes prevean estos requisitos.

3. 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 con arreglo al Reglamento (UE) 2019/881 y especificado con arreglo al apartado 4 son conformes con los requisitos esenciales establecidos en el anexo I en la medida en que la declaración UE de conformidad o el certificado de ciberseguridad, o partes de ellos, prevean dichos requisitos.

4. La Comisión estará facultada para especificar, mediante actos de ejecución, los esquemas europeos de certificación de la ciberseguridad adoptados con arreglo al Reglamento (UE) 2019/881 que puedan servir para demostrar la conformidad con los requisitos esenciales, o partes de ellos, establecidos en el anexo I. Además, cuando proceda, la Comisión especificará si un certificado de ciberseguridad expedido en el marco de dichos esquemas 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 24, apartado 2, letras a) y b), y apartado 3, letras a) y b). Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.

Artículo 19

Especificaciones comunes

Cuando no existan las normas armonizadas mencionadas en el artículo 18, cuando la Comisión considere que las normas armonizadas pertinentes son insuficientes para cumplir los requisitos del presente Reglamento o ajustarse a la petición de normalización de la Comisión, cuando se produzcan demoras indebidas en el procedimiento de normalización o cuando la solicitud de normas armonizadas por parte de la Comisión no haya sido aceptada por las organizaciones europeas de normalización, la Comisión estará facultada para adoptar, mediante actos de ejecución, especificaciones comunes con respecto a los requisitos esenciales establecidos en el anexo I. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.

Artículo 20

Declaración UE de conformidad

1. La declaración UE de conformidad será elaborada por los fabricantes con arreglo a lo dispuesto en el artículo 10, apartado 7, y hará constar que se ha demostrado el cumplimiento de los requisitos esenciales aplicables establecidos en el anexo I.

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

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

4. Al elaborar una declaración UE de conformidad, el fabricante asumirá la responsabilidad del cumplimiento por parte del producto.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de completar el presente Reglamento mediante la inclusión de elementos al contenido mínimo de la declaración UE de conformidad establecido en el anexo IV a fin de tener en cuenta los avances tecnológicos.

Artículo 21

Principios generales del marcado CE

El marcado CE, tal como se define en el artículo 3, punto 32, estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.

Artículo 22

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 20 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 20 o el sitio web que acompañen al producto.

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 especial establecido 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 24.

   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 el producto con elementos digitales esté sujeto a otras disposiciones legislativas de la Unión que también requieran la colocación del marcado CE, este indicará que el producto también cumple los requisitos de esas otras disposiciones legislativas.

6. La Comisión podrá, mediante actos de ejecución, establecer especificaciones técnicas para pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales, así como mecanismos para promover su uso. Dichos actos

de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.

Artículo 23

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 establecidos en el anexo I. Incluirá, como mínimo, los elementos establecidos en el anexo V.

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 durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto con elementos digitales en el mercado, si este período fuese más breve.

3. En el caso de los productos con elementos digitales a que se refieren el artículo 8 y el artículo 24, apartado 4, que también estén sujetos a otros actos de la Unión, se elaborará una única documentación técnica que contenga la información a que hace referencia el anexo V del presente Reglamento y la información requerida por esos actos de la Unión respectivos.

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 50 a fin de completar el presente Reglamento mediante la inclusión de elementos en la documentación técnica establecida en el anexo V a fin de tener en cuenta los avances tecnológicos, así como los imprevistos que surjan durante el proceso de ejecución del presente Reglamento.

Artículo 24

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 establecidos en el anexo I. El fabricante o su representante autorizado demostrarán la conformidad con los requisitos esenciales mediante uno de los procedimientos siguientes:

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

   b) procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VI, 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 VI; o

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

2. Cuando, al evaluar la conformidad del producto crítico 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 establecidos en el anexo I, el fabricante o su representante autorizado no haya aplicado o solo haya aplicado parcialmente las normas armonizadas, las especificaciones comunes o los esquemas europeos de certificación de la ciberseguridad a que se refiere el artículo 18, 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 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 VI, 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 VI; o

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

3. Cuando el producto sea un producto crítico con elementos digitales de la clase II según lo establecido en el anexo III, el fabricante o su representante autorizado demostrará la conformidad con los requisitos esenciales establecidos en el anexo I mediante uno de los procedimientos siguientes:

   a) procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VI, 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 VI; o

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

4. Los fabricantes de productos con elementos digitales considerados sistemas HME que entren en el ámbito de aplicación del Reglamento [Reglamento sobre el espacio europeo de datos sanitarios] demostrarán la conformidad con los requisitos esenciales establecidos en el anexo I del presente Reglamento mediante el procedimiento de evaluación de la conformidad pertinente exigido por el Reglamento [capítulo III del Reglamento sobre el espacio europeo de datos sanitarios].

5. Los organismos notificados tendrán en cuenta los intereses y las necesidades específicos de las pequeñas y medianas empresas (pymes) a la hora de fijar las tasas que aplican a los procedimientos de evaluación de la conformidad y reducirán dichas tasas de forma proporcionada a dichos intereses y necesidades específicos.

CAPÍTULO IV

NOTIFICACIÓN DE LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD

Artículo 25

Notificación

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

Artículo 26

Autoridades notificantes

1. Los Estados miembros designarán una autoridad notificante que será responsable de establecer y aplicar los procedimientos necesarios para la evaluación y notificación de los organismos de evaluación de la conformidad y para la supervisión de los organismos notificados, lo que incluye el cumplimiento del artículo 31.

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.

Artículo 27

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 ejercerá 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 28

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 esa información.

Artículo 29

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 que evalúen.

   Se puede considerar como organismos de evaluación de la conformidad a los organismos pertenecientes a una asociación comercial o una federación profesional que represente a las 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 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 será óbice para 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 comercialización, la instalación, el uso ni el mantenimiento de estos productos, 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 VI 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 efectúa 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 permitan distinguir entre las tareas efectuadas como organismo notificado y cualquier otra actividad;

c) de procedimientos para desempeñar 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.

Dispondrá de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrá acceso a todo el equipo o las instalaciones que necesite.

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 las normas armonizadas aplicables y de las disposiciones pertinentes de las normas de armonización de la Unión aplicables, así como de las normas de aplicación 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 el Estado 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 VI 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 40, o se asegurarán de que su personal de evaluación esté informado al respecto, y aplicarán a modo de

directrices 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 y razonables que tengan particularmente en cuenta los intereses de las pymes en relación con las tasas.

Artículo 30

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 29 en la medida en que las normas armonizadas aplicables cubran estos requisitos.

Artículo 31

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 29 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 32

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 para los cuales el organismo se considere competente, así como de un certificado de acreditación, si lo hay, 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 29.

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 29.

Artículo 33

Procedimiento de notificación

1. Las autoridades notificantes solo podrán notificar organismos de evaluación de la conformidad que hayan satisfecho los requisitos establecidos en el artículo 29.

2. La autoridad notificante pertinente enviará 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 (NANDO) 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 afectados y la correspondiente certificación de competencia.

4. Si la notificación no está basada en el certificado de acreditación a que se hace referencia en el artículo 32, 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 29.

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 34

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 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 35

Cambios en las notificaciones

1. Cuando una autoridad notificante compruebe que un organismo notificado ya no cumple los requisitos establecidos en el artículo 29 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 36

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 a los que esté sujeto.

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 37

Obligaciones operativas de los organismos notificados

1. Los organismos notificados realizarán evaluaciones de la conformidad siguiendo los procedimientos de evaluación de la conformidad establecidos en el artículo 24 y en el anexo VI.

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, 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.

3. Para ello respetarán, sin embargo, el grado de rigor y el nivel de protección requeridos para que el producto sea conforme con lo dispuesto en el presente Reglamento.

4. Si un organismo notificado comprueba 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 hace referencia en el artículo 19, 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 constata que el producto 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 el caso.

Artículo 38

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 información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de la evaluación de la conformidad.

Artículo 39

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 40

Coordinación de los organismos notificados

1. La Comisión se asegurará de que se instauren 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 41

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 que se encarguen de supervisar la aplicación eficaz 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. 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 con arreglo al artículo 11 del presente Reglamento, las autoridades de vigilancia del mercado designadas cooperarán con la ENISA.

4. Cuando corresponda, las autoridades de vigilancia del mercado cooperarán con otras autoridades de vigilancia del mercado designadas sobre la base de otras normas de armonización de la Unión para otros productos e intercambiarán información periódicamente.

5. 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 estas autoridades de toda constatación pertinente para el ejercicio de sus competencias, en particular al proporcionar orientaciones y asesoramiento con arreglo al apartado 8 del presente artículo, 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.

6. Los Estados miembros garantizarán que las autoridades de vigilancia del mercado designadas dispongan de recursos financieros y humanos adecuados para el desempeño de sus funciones con arreglo al presente Reglamento.

7. La Comisión facilitará el intercambio de experiencias entre las autoridades de vigilancia del mercado designadas.

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

9. 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.

10. 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

con arreglo al artículo [artículo 6] del Reglamento [Reglamento sobre IA], las autoridades de vigilancia del mercado designadas a efectos del Reglamento [Reglamento sobre IA] 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 con arreglo al Reglamento [Reglamento sobre IA] 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 11, con la ENISA. Las autoridades de vigilancia del mercado designadas con arreglo al Reglamento [Reglamento sobre IA] informarán, en particular, a las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento de toda constatación pertinente para el ejercicio de sus funciones en relación con la aplicación del presente Reglamento.

11. Se establecerá un Grupo de Cooperación Administrativa (ADCO) específico para la aplicación uniforme del presente Reglamento, de conformidad con el artículo 30, apartado 2, del Reglamento (UE) 2019/1020. Este 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.

Artículo 42

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 establecidos en el anexo I, se concederá a las autoridades de vigilancia del mercado, previa solicitud motivada, acceso a los datos 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 43

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 motivos suficientes para considerar que un producto con elementos digitales, en particular en lo que respecta a la gestión de las vulnerabilidades, presenta un riesgo de ciberseguridad significativo, efectuará 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 pertinente que adopte las medidas correctoras oportunas para llevar el producto a conformidad con los citados requisitos o bien retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo, que dicha autoridad 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 oportunas.

2. 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 a adoptar.

3. El fabricante 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.

4. Si el fabricante de un producto con elementos digitales 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 en su mercado nacional, para retirarlo de ese mercado o para recuperarlo.

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

5. La información mencionada en el apartado 4 incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación de los productos con elementos digitales no conformes, el origen del 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 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 establecidos en el anexo I por parte del producto o de los procesos establecidos por el fabricante;

   b) deficiencias en las normas armonizadas, esquemas de certificación de la ciberseguridad o especificaciones comunes a que hace referencia el artículo 18.

6. 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 en cuestión y, en caso de desacuerdo con la medida nacional notificada, sus objeciones al respecto.

7. Si, en el plazo de tres meses tras la recepción de la información indicada en el apartado 4, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por un Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador correspondiente con arreglo al artículo 18 del Reglamento (UE) 2019/1020.

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

Artículo 44

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 43, apartado 4, 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 43, apartado 4, si la medida nacional está justificada o no, y notificará dicha 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 10 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 18, la Comisión estudiará la posibilidad de modificar o derogar el acto de ejecución a que hace referencia el artículo 18, apartado 4, 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 19, la Comisión estudiará la posibilidad de modificar o derogar el acto de ejecución a que se hace referencia el artículo 19 por el que se establezcan dichas especificaciones comunes.

Artículo 45

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

1. Cuando la Comisión tenga motivos suficientes para considerar, en particular 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, podrá solicitar a las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hace referencia el artículo 43.

2. En circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto 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 podrá solicitar a la ENISA que lleve a cabo una evaluación del cumplimiento. 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.

3. Sobre la base de la evaluación de la ENISA, la Comisión podrá decidir sobre 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.

4. Sobre la base de la consulta a que hace referencia el apartado 3, la Comisión podrá adoptar actos de ejecución para decidir sobre medidas correctoras o restrictivas a escala de la Unión, como ordenar la retirada del mercado de los productos correspondientes o recuperarlos, en un plazo razonable, proporcional a la naturaleza del riesgo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que hace referencia el artículo 51, apartado 2.

5. La Comisión comunicará inmediatamente la decisión a que hace referencia el apartado 4 al operador u operadores económicos pertinentes. Los Estados miembros aplicarán los actos a que hace referencia el apartado 4 sin demora e informarán de ello a la Comisión.

6. Los apartados 2 a 5 serán aplicables mientras dure la situación excepcional que haya justificado la intervención de la Comisión y mientras el producto correspondiente no se lleve a conformidad con lo dispuesto en el presente Reglamento.

Artículo 46

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

1. Si, tras efectuar una evaluación con arreglo al artículo 43, la autoridad de vigilancia del mercado de un Estado miembro constata que un producto con elementos digitales y los procesos establecidos por el fabricante, a pesar de ser conformes con el presente Reglamento, presentan un riesgo de ciberseguridad significativo y, además, plantean un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones que impone el 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 de información electrónico por entidades esenciales del tipo contemplado en el [anexo I de la Directiva XXX/XXXX (SRI 2)] o para otros aspectos relativos a la protección del interés público, dicha autoridad exigirá al operador económico pertinente que adopte todas las medidas necesarias para garantizar que el producto con elementos digitales en cuestión y los procesos establecidos por el fabricante ya no presenten ese riesgo cuando se introduzca el producto en el mercado, o bien para retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo.

2. El fabricante u otros operadores 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 su decisión a los Estados miembros.

6. Cuando la Comisión tenga motivos suficientes para considerar, en particular 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, podrá solicitar a la autoridad o las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hacen referencia el artículo 43 y los apartados 1, 2 y 3 del presente artículo.

7. En circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto 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 podrá solicitar a la ENISA que lleve a cabo una evaluación de los riesgos que presenta el producto 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 de la ENISA a que hace referencia 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 pertinentes.

9. Sobre la base de la consulta a que hace referencia el apartado 8, la Comisión podrá adoptar actos de ejecución para decidir sobre medidas correctoras o restrictivas a escala de la Unión, como ordenar la retirada del mercado de los productos correspondientes o recuperarlos, en un plazo razonable, proporcional a la naturaleza del riesgo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que hace referencia el artículo 51, apartado 2.

10. La Comisión comunicará inmediatamente la decisión a que hace referencia el apartado 9 al operador u operadores pertinentes. Los Estados miembros aplicarán dichos actos 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 correspondiente siga presentando los riesgos a que hace referencia el apartado 1.

Artículo 47

Incumplimiento formal

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

   a) la colocación del marcado de conformidad no es conforme con los artículos 21 y 22;

   b) no se ha colocado el marcado de conformidad;

   c) no se ha redactado 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 48

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 que con frecuencia presentan riesgos de ciberseguridad.

2. La Comisión o la ENISA podrán proponer 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 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 resultante de las actividades 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 49

Barridos

1. Las autoridades de vigilancia del mercado podrán llevar 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.

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

3. En el desempeño de sus funciones, la ENISA podrá determinar, en particular sobre la base de las notificaciones recibidas de conformidad con el artículo 11, apartados 1

y 2, categorías de productos para las que puedan organizarse barridos. La propuesta de barrido se presentará al posible coordinador mencionado en el apartado 2 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 41 a 47 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 50

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. Se otorgarán a la Comisión los poderes para adoptar los actos delegados mencionados en el artículo 2, apartado 4, el artículo 6, apartados 2, 3 y 5, el artículo 20, apartado 5, y el artículo 23, apartado 5.

3. La delegación de poderes a que hacen referencia el artículo 2, apartado 4, el artículo 6, apartados 2, 3 y 5, el artículo 20, apartado 5, y el artículo 23, 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 la misma. 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 4, el artículo 6, apartados 2, 3 y 5, el artículo 20, apartado 5, y el artículo 23, 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 51

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, será aplicable 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 52

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 2016/943 del Parlamento Europeo y del Consejo[24];

   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.

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.

---

[24] 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).

Artículo 53

Sanciones

1. Los Estados miembros establecerán las normas sobre las sanciones aplicables a las infracciones del presente Reglamento cometidas por los operadores económicos y adoptarán todas las medidas necesarias para garantizar su ejecución. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias.

2. Los Estados miembros comunicarán sin demora a la Comisión esas normas y las medidas adoptadas y le notificarán sin demora cualquier modificación posterior que las afecte.

3. El incumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I y de las obligaciones establecidas en los artículos 10 y 11 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.

4. El incumplimiento de cualquier otra obligación establecida en el presente Reglamento estará sujeto 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.

5. La presentación de información incorrecta, incompleta o engañosa a organismos notificados y a las autoridades de vigilancia del mercado en respuesta a una solicitud estará sujeta a 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.

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

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

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

   c) el tamaño y la cuota de mercado del operador que comete la infracción.

7. Las autoridades de vigilancia del mercado que apliquen multas administrativas compartirán esta información con 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.

8. 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.

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

10. 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.

CAPÍTULO VIII

DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 54

Modificación del Reglamento (UE) 2019/1020

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

«71. [Reglamento XXX] [Ley de Ciberresiliencia]».

Artículo 55

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 otras normas de armonización de la Unión seguirán siendo válidos hasta el [cuarenta y dos meses después de 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 otras normas de la Unión, caso en el que seguirán siendo válidos según lo que dispongan dichas normas de la Unión.

2. Los productos con elementos digitales que hayan sido introducidos en el mercado antes del [fecha de aplicación del presente Reglamento especificada en el artículo 57] estarán sujetos a los requisitos del presente Reglamento únicamente si, a partir de dicha fecha, los productos mencionados se ven sometidos a modificaciones sustanciales en su diseño o su finalidad prevista.

3. No obstante lo dispuesto en el apartado 2, las obligaciones establecidas en el artículo 11 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 [fecha de aplicación del presente Reglamento especificada en el artículo 57].

Artículo 56

Evaluación y revisión

A más tardar el [treinta y seis meses después de 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.

Artículo 57

Entrada en vigor y aplicación

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

Será aplicable a partir del [veinticuatro meses después de la fecha de entrada en vigor del presente Reglamento]. No obstante, el artículo 11 será aplicable a partir del [doce meses después de la fecha de entrada en vigor del presente Reglamento].

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

Hecho en Bruselas, el

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

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Política(s) afectada(s)

1.3. La propuesta/iniciativa se refiere a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e incidencia esperados

1.4.4. Indicadores de rendimiento

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la aplicación de la iniciativa

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

1.6. Duración e incidencia financiera de la propuesta/iniciativa

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del(de los) modo(s) de gestión, el(los) mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos

2.2.2. Información relativa a los riesgos identificados y al / a los sistema(s) de control interno establecidos para atenuarlos

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

3.2.2. Resultados estimados financiados con créditos de operaciones

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Ley de Ciberresiliencia)

1.2. Política(s) afectada(s)

Redes de comunicación, contenido y tecnologías

1.3. La propuesta/iniciativa se refiere a:

× **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[37]

☐ **la prolongación de una acción existente**

☐ **una fusión o reorientación de una o más acciones hacia otra/una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

La propuesta tiene dos objetivos principales para garantizar el correcto funcionamiento del mercado interior: 1) **crear condiciones que permitan el desarrollo de productos con elementos digitales seguros**, garantizando que los productos de *hardware* y *software* 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; y 2) **crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utilizar productos con elementos digitales**.

1.4.2. Objetivo(s) específico(s)

Se establecieron **cuatro objetivos específicos** para la propuesta: i) garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida; ii) garantizar un marco de ciberseguridad coherente y facilitar su cumplimiento por parte de los productores de equipos y programas informáticos; iii) mejorar la transparencia de las características de seguridad de los productos con elementos digitales; y iv) permitir a las empresas y a los consumidores utilizar productos con elementos digitales de forma segura.

Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

La propuesta beneficiaría considerablemente a las distintas partes interesadas. Por lo que respecta a las empresas, evitaría la divergencia entre las normas de seguridad para los productos con elementos digitales y reduciría los costes de cumplimiento de

[37] Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero.

la legislación pertinente en materia de ciberseguridad. Reduciría el número de ciberincidentes, los costes de gestión de incidentes y el daño a la reputación. Para el conjunto de la UE, se calcula que la iniciativa podría dar lugar a una reducción de los costes derivados de los incidentes que afectan a las empresas de entre 180 000 y 290 000 millones EUR anuales aproximadamente[38]. Esto permitiría un aumento del consumo de productos con elementos digitales y, por tanto, del volumen de negocio. También mejoraría la reputación mundial de las empresas, lo que también daría lugar a un aumento de la demanda fuera de la UE. A nivel de los usuarios, la opción preferida aumentaría la transparencia de las propiedades de seguridad y facilitaría el uso de productos con elementos digitales. Los consumidores y los ciudadanos también se beneficiarían de una mejor protección de sus derechos fundamentales, como la privacidad y la protección de datos.

Al mismo tiempo, la propuesta añadiría costes de cumplimiento y de ejecución para las empresas, los organismos notificados y las autoridades públicas, incluidas las autoridades de acreditación y de vigilancia del mercado. Para los desarrolladores de programas informáticos y los fabricantes de equipos informáticos, añadirá costes directos de cumplimiento en relación con los nuevos requisitos de seguridad, la evaluación de la conformidad, la documentación y las obligaciones de información, lo que resultará en unos costes de cumplimiento agregados de hasta 29 000 millones EUR para un valor de mercado estimado de 1 485 000 millones EUR en volumen de negocio[39]. Es posible que los usuarios, incluidos los usuarios profesionales, los consumidores y los ciudadanos tengan que hacer frente a precios más elevados de los productos con elementos digitales. Sin embargo, estos costes deben considerarse en el contexto de los importantes beneficios descritos anteriormente.

1.4.3. Indicadores de rendimiento

Precisar los indicadores para hacer un seguimiento de los avances y logros.

Para comprobar si los fabricantes mejoran la seguridad de sus productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida de dichos productos, podrían tenerse en cuenta varios indicadores. Estos podrían ser el número de incidentes significativos en la Unión causados por vulnerabilidades, la proporción de fabricantes de equipos y programas informáticos que siguen un ciclo de vida del desarrollo seguro y sistemático, un análisis cualitativo de la seguridad de los productos con elementos digitales, una evaluación cuantitativa y cualitativa de las bases de datos de vulnerabilidades, la frecuencia de los parches de seguridad puestos a disposición por los fabricantes o el número medio de días entre el descubrimiento de la vulnerabilidad y el suministro de parches de seguridad.

Un indicador para un marco coherente en materia de ciberseguridad podría ser la ausencia de una legislación nacional en materia de ciberseguridad específica para cada producto.

---

38 Véase el [documento de trabajo de los servicios de la Comisión sobre el informe de evaluación de impacto que acompaña al Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales].

39 Véase el [documento de trabajo de los servicios de la Comisión sobre el informe de evaluación de impacto que acompaña al Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales].

Un indicador para una mayor transparencia en lo que respecta a las propiedades de seguridad de los productos con elementos digitales podría ser la proporción de productos con elementos digitales que se entregan acompañados de información sobre sus propiedades de seguridad. Además, la proporción de productos con elementos digitales que se entregan acompañados de instrucciones de uso seguro podría utilizarse como indicador de si las organizaciones y a los consumidores tienen la posibilidad de utilizar productos con elementos digitales de forma segura.

Por lo que se refiere al seguimiento de las repercusiones del Reglamento, se valorarán determinados indicadores a este respecto, que serán evaluados por la Comisión con, cuando proceda, el apoyo de la ENISA. En función del objetivo operativo que se deba alcanzar, algunos de los indicadores del seguimiento sobre cuya base se evaluaría el éxito de los requisitos horizontales de ciberseguridad son los siguientes:

Para evaluar el nivel de ciberseguridad de los productos con elementos digitales:

— Estadísticas y análisis cualitativos de incidentes que afectaron a productos con elementos digitales y la manera en que se gestionaron. La Comisión, con el apoyo de la ENISA, podría recopilar y evaluar estos datos.

— Registros de vulnerabilidades conocidas y análisis de su gestión. Este análisis podría correr a cargo de la ENISA, sobre la base de la base de datos europea de vulnerabilidades creada sobre la base de la [Directiva XXX/XXXX (SRI 2)].

— Encuestas entre los fabricantes de equipos y programas informáticos para supervisar los avances logrados.

Para evaluar el nivel de información sobre las medidas de seguridad, el apoyo en materia de seguridad, el final de la vida útil y el deber de diligencia: resultados de las encuestas que realizará la Comisión, con el apoyo de la ENISA, tanto entre los usuarios como entre las empresas.

Para evaluar la ejecución, la Comisión buscaría garantizar que las evaluaciones de la conformidad se lleven a cabo de manera eficaz. A tal fin, se formulará una petición de normalización y se hará un seguimiento de su ejecución. La Comisión también verificará la capacidad de los organismos notificados y, en su caso, de los organismos de certificación.

En lo que respecta a la aplicación, la Comisión comprobará, por medio de los informes de los Estados miembros, que las iniciativas nacionales no aborden aspectos que entren en el ámbito de aplicación del Reglamento.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la aplicación de la iniciativa

El Reglamento debe ser plenamente aplicable veinticuatro meses después de su entrada en vigor. No obstante, deben establecerse determinados elementos de la estructura de gobernanza con anterioridad. En particular, los Estados miembros deberán haber designado con anterioridad a autoridades existentes o establecido nuevas autoridades para desempeñar las funciones previstas en la legislación.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

La importante naturaleza transfronteriza de la ciberseguridad y el aumento de los incidentes, cuyas repercusiones pueden extenderse a otros países, sectores y productos, hacen que los Estados miembros por sí solos no puedan alcanzar eficazmente los objetivos planteados. Habida cuenta de la dimensión mundial de los mercados de los productos con elementos digitales, los Estados miembros hacen frente en su territorio a los mismos riesgos para un mismo producto con elementos digitales. El mosaico de normas nacionales con posibles divergencias que está surgiendo corre el riesgo de poner barreras a un mercado único abierto y competitivo para los productos con elementos digitales. Por lo tanto, se hace necesaria la acción conjunta a escala de la UE para aumentar el nivel de confianza entre los usuarios y el atractivo de los productos con elementos digitales de la UE. La acción conjunta también beneficiaría al mercado interior al proporcionar seguridad jurídica y condiciones de competencia equitativas para los vendedores de productos con elementos digitales.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La Ley de Ciberresiliencia es el primer reglamento de este tipo en introducir requisitos de ciberseguridad para la introducción de productos con elementos digitales en el mercado. No obstante, se fundamenta en el establecimiento del nuevo marco legislativo y en las lecciones aprendidas en el proceso de ejecución de la legislación de armonización de la Unión vigente en relación con diversos productos, en particular en lo que se refiere a la preparación para la ejecución, incluidos aspectos como la preparación de normas armonizadas.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

El Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales define nuevos requisitos de ciberseguridad para todos los productos con elementos digitales introducidos en el mercado de la UE, que van más allá de los requisitos establecidos en la legislación vigente. Al mismo tiempo, la propuesta se basa en la actual configuración del nuevo marco legislativo. Se basaría por tanto en las estructuras y procedimientos existentes del nuevo marco legislativo, como la cooperación de los organismos notificados y la vigilancia del mercado, los módulos de evaluación de la conformidad y el desarrollo de normas armonizadas. La nueva propuesta se basaría también en algunas estructuras establecidas con arreglo a otra legislación en materia de ciberseguridad, como la Directiva 2016/1148 (Directiva SRI), la [Directiva XXX/XXXX (SRI 2)] o el Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad), respectivamente.

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

La gestión de los ámbitos de actuación asignados a la ENISA se ajusta a su actual mandato y funciones generales. Estos ámbitos de actuación pueden requerir perfiles específicos o nuevas asignaciones, pero estos no serían de una exigencia particular y

podrían ser absorbidos por los recursos existentes de la ENISA y resolverse mediante la reasignación o la vinculación de varias asignaciones. Por ejemplo, uno de los principales ámbitos de actuación asignados a la ENISA se refiere a la recopilación y el tratamiento de las notificaciones de los fabricantes relativas a las vulnerabilidades aprovechadas de los productos. La [Directiva XXX/XXXX (SRI 2)] ya ha encargado a la ENISA la creación de una base de datos europea de vulnerabilidades en la que puedan divulgarse y registrarse de forma voluntaria vulnerabilidades conocidas públicamente, con el fin de permitir a los usuarios adoptar las medidas paliativas oportunas. Los recursos asignados a tal efecto también podrían utilizarse para las nuevas asignaciones antes mencionadas relativas a las notificaciones de vulnerabilidades de los productos. Esta reasignación podría garantizar un uso eficaz de los recursos existentes y crearía también las sinergias necesarias entre las misiones que puedan orientar mejor los análisis de los riesgos y amenazas para la ciberseguridad que la ENISA lleve a cabo.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

– ☐ en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA

– ☐ incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.

× **duración ilimitada**

– Ejecución con una fase de puesta en marcha a partir de 2025,

– y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[40]

☐ **Gestión directa a cargo** de la Comisión

– × por sus departamentos, incluido su personal en las delegaciones de la Unión;

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especifíquense);

– ☐ el BEI y el Fondo Europeo de Inversiones;

– ☐ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

– ☐ organismos de Derecho público;

– ☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

– ☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

Observaciones

El presente Reglamento asigna determinadas acciones a la ENISA, de conformidad con su actual mandato, y en particular con el artículo 3, apartado 2, del Reglamento (UE) 2019/881, que dispone que la ENISA debe desempeñar los cometidos que le confieran los actos jurídicos de la Unión que establezcan medidas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de ciberseguridad. En particular, la ENISA es la encargada de recibir notificaciones de los fabricantes relativas a las

[40] La información sobre los modos de gestión y las referencias al Reglamento Financiero puede consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

vulnerabilidades aprovechadas activamente presentes en los productos con elementos digitales, así como a los incidentes que repercutan en la seguridad de dichos productos. La ENISA también debe transmitir estas notificaciones a los CSIRT pertinentes o, según corresponda, al punto de contacto único pertinente designado de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como informar a las autoridades de vigilancia del mercado. 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 SRI. Además, teniendo en cuenta los conocimientos técnicos de la ENISA, la información recopilada y los análisis de amenazas, la ENISA podrá apoyar el proceso de ejecución del presente Reglamento mediante la propuesta de actividades conjuntas que las autoridades nacionales de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre el posible incumplimiento del presente Reglamento por parte de productos con elementos digitales en varios Estados miembros, o identificar categorías de productos para las que puedan organizarse acciones de control simultáneas coordinadas. La Comisión podrá solicitar a la ENISA que, en circunstancias excepcionales, lleve a cabo evaluaciones de productos específicos con elementos digitales que presenten un riesgo de ciberseguridad significativo, siempre que sea necesaria una intervención inmediata para preservar el buen funcionamiento del mercado interior.

Se estima que estas misiones, en su conjunto, requieran que la ENISA dedique alrededor de 4,5 EJC de sus recursos existentes, aprovechando los conocimientos especializados y el trabajo preparatorio que la ENISA ya realiza actualmente, entre otras cosas, en apoyo de la futura ejecución de la [Directiva XXX/XXXX (SRI 2)], para la que se han asignado recursos adicionales a la ENISA.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

A más tardar treinta y seis meses después de que el presente Reglamento sea aplicable, 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.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del(de los) modo(s) de gestión, el(los) mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos

El presente Reglamento establece una nueva política con respecto a los requisitos de ciberseguridad armonizados para los productos con elementos digitales introducidos en el mercado interior a lo largo de todo su ciclo de vida. El acto jurídico irá seguido de solicitudes de la Comisión a los organismos europeos de normalización para que elaboren normas.

Para que puedan afrontar estas tareas, es necesario dotar de recursos apropiados a los servicios de la Comisión. Se calcula que la aplicación del nuevo Reglamento requiere 7 EJC (de los cuales 1 ENCS) para desempeñar las siguientes tareas:

- preparar la petición de normalización o las especificaciones comunes a través de un proceso de normalización satisfactorio en el que no medien actos de ejecución;
- preparar un acto delegado [en un plazo de doce meses a partir de la entrada en vigor del Reglamento] en el que se especifiquen las definiciones de los productos críticos con elementos digitales;
- preparar, si procede, actos delegados para actualizar la lista de productos críticos de las clases I y II; especificar si es necesario limitar o excluir los productos con elementos digitales regulados por otras normas de la Unión en las que se establecen requisitos que ofrecen el mismo nivel de protección que el Reglamento propuesto; exigir la certificación de determinados productos altamente críticos con elementos digitales sobre la base de los criterios establecidos en el Reglamento, especificar el contenido mínimo de la declaración de conformidad de la UE y completar los elementos que deban incluirse en la documentación técnica;
- preparar, si procede, actos de ejecución relativos al formato o a los elementos de las obligaciones de información, la nomenclatura de materiales de los programas informáticos, las especificaciones comunes o la colocación del marcado CE;
- preparar, si procede, una intervención inmediata en circunstancias excepcionales para imponer medidas correctoras o restrictivas a fin de preservar el buen funcionamiento del mercado interior, incluida la preparación de un acto de ejecución;
- organizar y coordinar las notificaciones de los Estados miembros relativas a los organismos notificados, y coordinar dichos organismos;

– apoyar la coordinación de las autoridades de vigilancia del mercado de los Estados miembros.

2.2.2. Información relativa a los riesgos identificados y al / a los sistema(s) de control interno establecidos para atenuarlos

Para garantizar que los organismos notificados y las autoridades de vigilancia del mercado intercambien información y cooperen de manera correcta, la Comisión es responsable de su coordinación. En relación con los conocimientos técnicos y del mercado, se crearía un grupo de expertos.

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

2.3. En lo relativo a los gastos de reuniones, debido al reducido valor por transacción (p. ej., el reembolso de los gastos de viaje de un delegado que participe en una reunión), los procedimientos de control normalizados parecen suficientes. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

Las medidas existentes de prevención del fraude aplicables a la Comisión cubrirán los créditos adicionales necesarios para el presente Reglamento.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias existentes

Esquema

- Nuevas líneas presupuestarias solicitadas

No aplicable

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

– ☑ La propuesta/iniciativa no exige la utilización de créditos de operaciones

– ☐ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	

DG: <…….>			Año **N**[41]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
• Créditos de operaciones										
Línea presupuestaria[42]	Compromisos	(1a)								
	Pagos	(2a)								
Línea presupuestaria	Compromisos	(1b)								
	Pagos	(2b)								
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[43]										
Línea presupuestaria		(3)								
TOTAL de los créditos	Compromisos	= 1a + 1b + 3								

41 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación previsto (por ejemplo: 2021). Hágase lo mismo con los años siguientes.

42 Según la nomenclatura presupuestaria oficial.

43 Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

para la DG <…….>	Pagos	= 2a + 2b + 3								

• TOTAL de los créditos de operaciones	Compromisos	(4)								
	Pagos	(5)								
•TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)								
TOTAL de los créditos para la RÚBRICA <….> del marco financiero plurianual	Compromisos	= 4 + 6								
	Pagos	= 5 + 6								

Si la propuesta/iniciativa afecta a más de una línea operativa, repetir la sección anterior:

• TOTAL de los créditos de operaciones (todas las líneas operativas)	Compromisos	(4)								
	Pagos	(5)								
TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos (todas las líneas operativas)		(6)								
TOTAL de los créditos para las RÚBRICAS 1 a 6 del marco financiero plurianual (Importe de referencia)	Compromisos	= 4 + 6								
	Pagos	= 5 + 6								

Rúbrica del marco financiero plurianual	7	«Gastos administrativos»

Esta sección debe rellenarse mediante «los datos presupuestarios de carácter administrativo» introducidos primeramente en el anexo de la ficha financiera legislativa (anexo V de las normas internas), que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
DG: CNECT						
• Recursos humanos		1,030	1,030	1,030	1,030	**4,120**
• Otros gastos administrativos		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTAL para la DG CNECT	Créditos	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTAL de los créditos para la RÚBRICA 7 del marco financiero plurianual	(Total de los créditos de compromiso = total de los créditos de pago)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

En millones EUR (al tercer decimal)

		Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 7 del marco financiero plurianual	Compromisos	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Pagos	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Resultados estimados financiados con créditos de operaciones

Créditos de compromiso en millones EUR (al tercer decimal)

Indicar los objetivos y los resultados			Año **N**		Año **N+1**		Año **N+2**		Año **N+3**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
	RESULTADOS																	
⇩	Tipo[44]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.° 1[45]…																		
— Resultado																		
— Resultado																		
— Resultado																		
Subtotal del objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2...																		
— Resultado																		
Subtotal del objetivo específico n.º 2																		
TOTALES																		

[44] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[45] Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

– ☐ La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo.

– ☑ La propuesta/iniciativa exige la utilización de créditos de carácter administrativo, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2024**	Año **2025**	Año **2026**	Año **2027**	
RÚBRICA 7 del marco financiero plurianual					
Recursos humanos	1,030	1,030	1,030	1,030	**4,120**
Otros gastos administrativos	0,222	0,222	0,222	0,222	**0,888**
Subtotal para la RÚBRICA 7 del marco financiero plurianual	1,252	1,252	1,252	1,252	**5,008**

Al margen de la RÚBRICA 7[46] del marco financiero plurianual					
Recursos humanos					
Otros gastos de carácter administrativo					
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual					

TOTAL	1,252	1,252	1,252	1,252	**5,008**

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción y/o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

[46] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.3.1. Necesidades estimadas en recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– ☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

		Año **2024**	Año **2025**	Año **2026**	Año **2027**
20 01 02 01 (Sedes y Oficinas de Representación de la Comisión)		6	6	6	6
20 01 02 03 (Delegaciones)					
01 01 01 01 (investigación indirecta)					
01 01 01 11 (Investigación directa)					
Otras líneas presupuestarias (especifíquense)					
• **Personal externo (en unidades de equivalente a jornada completa: EJC)**[47]					
20 02 01 (AC, ENCS, INT de la dotación global)		1	1	1	1
20 02 03 (AC, AL, ENCS, INT y JPD en las Delegaciones)					
XX 01 xx **yy zz** [48]	— en la sede				
	— en las delegaciones				
01 01 01 02 (AC, ENCS, INT; investigación indirecta)					
01 01 01 12 (AC, INT, ENCS; investigación directa)					
Otras líneas presupuestarias (especifíquense)					
TOTAL		**7**	**7**	**7**	**7**

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales 6 FTE x 157 000 EUR/año = 942 000 EUR	Tal como se describe en el punto 2.2.1.: – preparar la petición de normalización o las especificaciones comunes a través de un proceso de normalización satisfactorio en el que no medien actos de ejecución; – preparar un acto delegado [en un plazo de doce meses a partir de la entrada en vigor del Reglamento] en el que se especifiquen las definiciones de los productos críticos con elementos digitales; – preparar, si procede, actos delegados para actualizar la lista de productos críticos de las clases I y II; especificar si es necesario limitar o excluir los productos con elementos digitales regulados por otras normas de la Unión en las que se establecen requisitos que ofrecen el mismo nivel de protección que el Reglamento propuesto; exigir la certificación de determinados productos altamente críticos con elementos digitales sobre la base de los criterios establecidos en el Reglamento; especificar el contenido mínimo de la declaración de conformidad de la UE y completar los elementos que

[47] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD = joven profesional en las Delegaciones.

[48] Subtecho para el personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

	deban incluirse en la documentación técnica; – preparar, si procede, actos de ejecución relativos al formato o a los elementos de las obligaciones de información, la nomenclatura de materiales de los programas informáticos, las especificaciones comunes o la colocación del marcado CE; – preparar, si procede, una intervención inmediata en circunstancias excepcionales para imponer medidas correctoras o restrictivas a fin de preservar el buen funcionamiento del mercado interior, incluida la preparación de un acto de ejecución; – organizar y coordinar las notificaciones de los Estados miembros relativas a los organismos notificados, y coordinar dichos organismos; – apoyar la coordinación de las autoridades de vigilancia del mercado de los Estados miembros.
Personal externo 1 ENCS x 88 000 EUR/año	Tal como se describe en el punto 2.2.1.: – preparar la petición de normalización o las especificaciones comunes a través de un proceso de normalización satisfactorio en el que no medien actos de ejecución; – preparar un acto delegado [en un plazo de doce meses a partir de la entrada en vigor del Reglamento] en el que se especifiquen las definiciones de los productos críticos con elementos digitales; – preparar, si procede, actos delegados para actualizar la lista de productos críticos de las clases I y II; especificar si es necesario limitar o excluir los productos con elementos digitales regulados por otras normas de la Unión en las que se establecen requisitos que ofrecen el mismo nivel de protección que el Reglamento propuesto; exigir la certificación de determinados productos altamente críticos con elementos digitales sobre la base de los criterios establecidos en el Reglamento; especificar el contenido mínimo de la declaración de conformidad de la UE y completar los elementos que deban incluirse en la documentación técnica; – preparar, si procede, actos de ejecución relativos al formato o a los elementos de las obligaciones de información, la nomenclatura de materiales de los programas informáticos, las especificaciones comunes o la colocación del marcado CE; – preparar, si procede, una intervención inmediata en circunstancias excepcionales para imponer medidas correctoras o restrictivas a fin de preservar el buen funcionamiento del mercado interior, incluida la preparación de un acto de ejecución; – organizar y coordinar las notificaciones de los Estados miembros relativas a los organismos notificados, y coordinar dichos organismos; – apoyar la coordinación de las autoridades de vigilancia del mercado de los Estados miembros.

3.2.4. Compatibilidad con el marco financiero plurianual vigente

La propuesta/iniciativa:

– x puede ser financiada en su totalidad mediante una redistribución dentro de la rúbrica correspondiente del marco financiero plurianual (MFP).

No es necesaria una reprogramación.

– ☐ requiere el uso de los márgenes no asignados con cargo a la rúbrica correspondiente del MFP o el uso de instrumentos especiales tal como se define en el Reglamento del MFP.

-

– ☐ requiere una revisión del MFP.

-

3.2.5. Contribución de terceros

La propuesta/iniciativa:

– x no prevé la cofinanciación por terceros

– ☐ prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**[49]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

[49] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación previsto (por ejemplo: 2021). Hágase lo mismo con los años siguientes.

3.3. Incidencia estimada en los ingresos

– ☐ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ en los recursos propios

– ☐ en otros ingresos

– indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[50]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo …….								

En el caso de los ingresos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

Otras observaciones (por ejemplo, método/fórmula que se utiliza para calcular la incidencia en los ingresos o cualquier otra información).

[50] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 20 % de los gastos de recaudación.