►B **REGLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

de 23 de octubre de 2024

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

(Texto pertinente a efectos del EEE)

(DO L 2847 de 20.11.2024, p. 1)

Rectificado por:

►C1 Rectificación, DO L 90555 de 2.7.2025, p. 1 (2024/2847)
►C2 Rectificación, DO L 90828 de 17.10.2025, p. 1 (2024/2847)

▼B

REGLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 23 de octubre de 2024

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

(Texto pertinente a efectos del EEE)

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

El presente Reglamento establece:

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

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

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

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

Artículo 2

Ámbito de aplicación

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

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

a) el Reglamento (UE) 2017/745;

b) el Reglamento (UE) 2017/746;

c) el Reglamento (UE) 2019/2144.

▼B

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

4. El presente Reglamento no es aplicable a los equipos que entran en el ámbito de aplicación de la Directiva 2014/90/UE del Parlamento Europeo y del Consejo ([1]).

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

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

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

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

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

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

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

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

Artículo 4

Libre circulación

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

▼B

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

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

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

Artículo 5

Contratación pública o uso de productos con elementos digitales

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

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

Artículo 6

Requisitos aplicables a los productos con elementos digitales

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

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

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

▼B

Artículo 7

Productos importantes con elementos digitales

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

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

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

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

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

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

4. A más tardar el 11 de diciembre de 2025, la Comisión adoptará un acto de ejecución que especifique la descripción técnica de las categorías de productos con elementos digitales de las clases I y II establecidas en el anexo III y la descripción técnica de las categorías de productos con elementos digitales establecidas en el anexo IV. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 62, apartado 2.

▼B

Artículo 8

Productos críticos con elementos digitales

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

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

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

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

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

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

▼B

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

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

Artículo 9

Consultas con las partes interesadas

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

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

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

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

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

Artículo 10

Refuerzo de las competencias en un entorno digital ciberresiliente

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

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

▼B

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

Artículo 11

Seguridad general de los productos

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

Artículo 12

Sistemas de IA de alto riesgo

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

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

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

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

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

▼B

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

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

CAPÍTULO II

OBLIGACIONES DE LOS OPERADORES ECONÓMICOS Y DISPOSICIONES RELATIVAS A LOS PROGRAMAS INFORMÁTICOS LIBRES Y DE CÓDIGO ABIERTO

Artículo 13

Obligaciones de los fabricantes

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

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

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

▼B

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

▼B

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

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

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

Artículo 14

Obligaciones de información de los fabricantes

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

iii) las medidas paliativas aplicadas y en curso.

▼B

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

9. A más tardar 11 de diciembre de 2025, la Comisión adoptará actos delegados de conformidad con el artículo 61 del presente Reglamento para completar el presente Reglamento mediante la especificación de las condiciones de aplicación de los motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de notificaciones a que se refiere el artículo 16, apartado 2, del presente Reglamento. La Comisión cooperará con la red de CSIRT establecida en virtud del artículo 15 de la Directiva (UE) 2022/2555 y con la ENISA en la preparación de los proyectos de actos delegados.

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

Artículo 15

Notificación voluntaria

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

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

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

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

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

▼B

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

Artículo 16

Creación de una plataforma única de notificación

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

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

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

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

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

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

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

▼B

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

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

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

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

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

▼B

Artículo 17

Otras disposiciones relativas a las notificaciones

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

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

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

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

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

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

Artículo 18

Representantes autorizados

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

▼B

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

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

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

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

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

Artículo 19

Obligaciones de los importadores

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

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

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

b) el fabricante ha redactado la documentación técnica;

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

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

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

▼B

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

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

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

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

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

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

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

▼B

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

Artículo 20

Obligaciones de los distribuidores

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

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

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

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

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

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

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

▼B

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

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

Artículo 21

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

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

Artículo 22

Otros casos en que son aplicables las obligaciones de los fabricantes

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

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

Artículo 23

Identificación de los operadores económicos

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

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

▼B

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

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

Artículo 24

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

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

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

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

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

Artículo 25

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

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

▼B

Artículo 26

Orientaciones

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

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

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

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

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

d) el concepto de modificación sustancial.

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

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

CAPÍTULO III

CONFORMIDAD DEL PRODUCTO CON ELEMENTOS DIGITALES

Artículo 27

Presunción de conformidad

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

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

▼B

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

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

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

   i) la solicitud no haya sido aceptada,

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

   iii) las normas armonizadas no se ajusten a la solicitud, y

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

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

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

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

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

6. Cuando un organismo europeo de normalización adopte una norma armonizada y la proponga a la Comisión con el fin de publicar su referencia en el *Diario Oficial de la Unión Europea*, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando se publique la referencia de una norma armonizada en el *Diario Oficial de la Unión Europea*, la Comisión derogará los actos de ejecución a que se refiere el apartado 2, o las partes de estos que se refieran a los mismos requisitos esenciales de ciberseguridad regulados que sean objeto de dicha norma armonizada.

▼B

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

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

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

Artículo 28

Declaración UE de conformidad

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

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

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

▼B

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

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

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

Artículo 29

Principios generales del marcado CE

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

Artículo 30

Reglas y condiciones para la colocación del marcado CE

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

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

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

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

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

▼B

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

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

Artículo 31

Documentación técnica

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

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

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

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

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

▼B

Artículo 32

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

Artículo 33

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

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

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

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

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

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

▼B

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

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

5. Las microempresas y las pequeñas empresas podrán facilitar todos los elementos de la documentación técnica especificada en el anexo VII utilizando un formato simplificado. A tal fin, la Comisión especificará, mediante actos de ejecución, el formulario simplificado de documentación técnica dirigido a las necesidades de las microempresas y las pequeñas empresas, incluida la forma en que deben facilitarse los elementos establecidos en el anexo VII. Cuando una microempresa o pequeña empresa opte por facilitar la información establecida en el anexo VII de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

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

Artículo 34

Acuerdos de reconocimiento mutuo

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

CAPÍTULO IV

NOTIFICACIÓN DE LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD

Artículo 35

Notificación

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

2. Los Estados se esforzarán por garantizar, a más tardar el 11 de diciembre de 2026, que haya un número suficiente de organismos notificados en la Unión para llevar a cabo evaluaciones de la conformidad, con objeto de evitar cuellos de botella y obstáculos para el acceso al mercado.

▼B

Artículo 36

Autoridades notificantes

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

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

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

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

Artículo 37

Requisitos relativos a las autoridades notificantes

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

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

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

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

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

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

Artículo 38

Obligación de información de las autoridades notificantes

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

▼B

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

Artículo 39

Requisitos relativos a los organismos notificados

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

Artículo 40

Presunción de conformidad de los organismos notificados

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

Artículo 41

Subcontrataciones y filiales de los organismos notificados

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

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

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

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

▼B

Artículo 42

Solicitud de notificación

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

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

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

Artículo 43

Procedimiento de notificación

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

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

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

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

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

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

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

▼B

Artículo 44

Números de identificación y listas de organismos notificados

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

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

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

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

Artículo 45

Cambios en las notificaciones

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

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

Artículo 46

Cuestionamiento de la competencia de los organismos notificados

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

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

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

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

▼B

Artículo 47

Obligaciones operativas de los organismos notificados

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

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

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

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

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

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

Artículo 48

Recurso frente las decisiones de los organismos notificados

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

Artículo 49

Obligación de información de los organismos notificados

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

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

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

▼B

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

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

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

Artículo 50

Intercambio de experiencias

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

Artículo 51

Coordinación de los organismos notificados

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

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

CAPÍTULO V

VIGILANCIA DEL MERCADO Y APLICACIÓN DE LA LEGISLACIÓN

Artículo 52

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

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

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

▼B

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

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

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

Artículo 53

Acceso a datos y documentación

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

Artículo 54

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

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

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

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

Artículo 55

Procedimiento de salvaguardia de la Unión

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

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

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

▼B

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

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

Artículo 56

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

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

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

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

▼B

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

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

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

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

Artículo 57

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

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

a) la salud o la seguridad de las personas;

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

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

Artículo 58

Incumplimiento formal

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

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

b) no se ha colocado el marcado CE;

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

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

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

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

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

Artículo 59

Actividades conjuntas de las autoridades de vigilancia del mercado

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

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

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

▼B

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

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

Artículo 60

Barridos

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

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

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

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

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

CAPÍTULO VI

PODERES DELEGADOS Y PROCEDIMIENTO DE COMITÉ

Artículo 61

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados mencionados en el artículo 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 y 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, y en el artículo 31, apartado 5, se otorgan a la Comisión por un período de cinco años a partir del 10 de diciembre de 2024. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

▼B

3. La delegación de poderes a que hacen referencia el artículo 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 y 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, y el artículo 31, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 2, apartado 5, párrafo segundo, el artículo 7, apartado 3, el artículo 8, apartados 1 o 2, el artículo 13, apartado 8, párrafo cuarto, el artículo 14, apartado 9, el artículo 25, el artículo 27, apartado 9, el artículo 28, apartado 5, o el artículo 31, apartado 5, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo mencionado se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 62

Procedimiento de comité

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

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

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

CAPÍTULO VII

CONFIDENCIALIDAD Y SANCIONES

Artículo 63

Confidencialidad

1. Todas las partes involucradas en la aplicación del presente Reglamento respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, en particular:

▼B

a) los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de las personas físicas o jurídicas, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo ([1]);

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.

Artículo 64

Sanciones

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

10. ►C1 Como excepción a lo dispuesto en los apartados 2 a 9, las multas administrativas a que se refieren esos apartados no se aplicarán a: ◄

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

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

▼B

Artículo 65

Acciones de representación

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

CAPÍTULO VIII

DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 66

Modificación del Reglamento (UE) 2019/1020

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

«72. Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo (*).

(*) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).».

Artículo 67

Modificación de la Directiva (UE) 2020/1828

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

▼C2

«72) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo (*).

▼B

(*) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).»

Artículo 68

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

El anexo II del Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo ([5]) se modifica como sigue:En el cuadro de la parte C1, se añade la entrada siguiente:

«

16	18	Protección del vehículo frente a ciberataques		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

»

▼B

Artículo 69

Disposiciones transitorias

1. Los certificados de examen de tipo UE y las decisiones de aprobación expedidos en relación con los requisitos de ciberseguridad para productos con elementos digitales que estén sujetos a otra legislación de armonización de la Unión distintas del presente Reglamento seguirán siendo válidos hasta el 11 de junio de 2028, salvo que caduquen con anterioridad a esa fecha o salvo que se indique lo contrario en esa legislación de armonización de la Unión, en cuyo caso seguirán siendo válidos según lo que disponga dicha legislación de la Unión.

2. Los productos con elementos digitales que hayan sido introducidos en el mercado antes del 11 de diciembre de 2027 estarán sujetos a los requisitos establecidos en el presente Reglamento únicamente si, a partir de dicha fecha, los productos mencionados se ven sometidos a una modificación sustancial.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, las obligaciones establecidas en el artículo 14 se aplicarán a todos los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento y hayan sido introducidos en el mercado antes del 11 de diciembre de 2027.

Artículo 70

Evaluación y revisión

1. A más tardar el 11 de diciembre de 2030, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

2. A más tardar el 11 de septiembre de 2028, la Comisión, previa consulta a la ENISA y a la red de CSIRT, presentará un informe al Parlamento Europeo y al Consejo en el que se evalúe la eficacia de la plataforma única de notificación establecida en el artículo 16, así como las repercusiones de la aplicación de los motivos relacionados con la ciberseguridad a que se refiere el artículo 16, apartado 2, por parte de los CSIRT designados como coordinadores en la eficacia de la plataforma única de notificación en lo que respecta a la difusión oportuna de las notificaciones recibidas a otros CSIRT pertinentes.

Artículo 71

Entrada en vigor y aplicación

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

2. El presente Reglamento será aplicable a partir del 11 de diciembre de 2027.

No obstante, el artículo 14 será aplicable a partir del 11 de septiembre de 2026 y el capítulo IV (artículos 35 a 51) será aplicable a partir del 11 de junio de 2026.

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

▼B

ANEXO I

REQUISITOS ESENCIALES DE CIBERSEGURIDAD

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

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

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

   a) se comercializarán sin vulnerabilidades aprovechables conocidas;

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

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

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

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

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

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

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

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

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

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

▼B

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

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

Parte II Requisitos de gestión de las vulnerabilidades

Los fabricantes de los productos con elementos digitales:

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

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

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

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

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

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

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

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

▼B

ANEXO II

INFORMACIÓN E INSTRUCCIONES PARA EL USUARIO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

ANEXO III

PRODUCTOS IMPORTANTES CON ELEMENTOS DIGITALES

Clase I

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

2. Navegadores independientes e integrados

3. Gestores de contraseñas

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

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

6. Sistemas de gestión de redes

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

8. Gestores de arranque

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

10. Interfaces físicas y virtuales de red

11. Sistemas operativos

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

13. Microprocesadores con funcionalidades relacionadas con la seguridad

14. Microcontroladores con funcionalidades relacionadas con la seguridad

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

16. Asistentes virtuales de propósito general para hogares inteligentes

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

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

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

Clase II

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

2. Cortafuegos y sistemas de detección y prevención de intrusiones

3. Microprocesadores resistentes a las manipulaciones

4. Microcontroladores resistentes a las manipulaciones.

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

▼B

ANEXO IV

PRODUCTOS CRÍTICOS CON ELEMENTOS DIGITALES

1. Dispositivos de equipos informáticos con cajas de seguridad

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

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

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

▼B

ANEXO V

DECLARACIÓN UE DE CONFORMIDAD

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

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

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

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

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

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

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

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

8. Información adicional:

   Firmado por y en nombre de:

   (lugar y fecha de expedición):

   (nombre, cargo) (firma):

▼B

ANEXO VI

DECLARACIÓN UE DE CONFORMIDAD SIMPLIFICADA

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

Por la presente, … [nombre del fabricante] declara que el tipo de producto con elementos digitales [designación del tipo de producto con elemento digital] es conforme con el Reglamento (UE) 2024/2847 ([1]).

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

([1]) DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

▼B

ANEXO VII

CONTENIDO DE LA DOCUMENTACIÓN TÉCNICA

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

1. una descripción general del producto con elementos digitales, incluidas:
   a) su finalidad prevista;
   b) las versiones de los programas informáticos que afecten al cumplimiento de los requisitos esenciales de ciberseguridad;
   c) cuando el producto con elementos digitales sea un producto consistente en equipos informáticos, fotografías o ilustraciones que muestren las características externas, el marcado y la configuración interna;
   d) la información y las instrucciones para el usuario indicadas en el anexo II;
2. una descripción del diseño, el desarrollo y la producción del producto con elementos digitales y de los procesos de gestión de las vulnerabilidades, que incluya:
   a) información necesaria sobre el diseño y el desarrollo del producto con elementos digitales, incluidos, en su caso, planos y esquemas, y una descripción de la arquitectura del sistema que explique cómo se apoyan o se alimentan mutuamente los componentes de los programas informáticos y cómo se integran en el tratamiento general;
   b) información y especificaciones necesarias de los procesos de gestión de las vulnerabilidades establecidos por el fabricante, incluida la nomenclatura de materiales de los programas informáticos, la política de divulgación coordinada de vulnerabilidades, pruebas de que se ha facilitado una dirección de contacto para la notificación de vulnerabilidades y una descripción de las soluciones técnicas elegidas para la distribución segura de las actualizaciones;
   c) información y especificaciones necesarias de los procesos de producción y seguimiento del producto con elementos digitales y la validación de esos procesos;
3. una evaluación de los riesgos de ciberseguridad frente a los cuales se haya diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, en virtud del artículo 13, también en lo que ataña al modo en que son aplicables los requisitos esenciales de ciberseguridad formulados en el anexo I, parte I;
4. información pertinente que se haya tenido en cuenta para determinar el período de soporte en virtud del artículo 13, apartado 8, del producto con elementos digitales;
5. una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, las especificaciones comunes tal como se definen en el artículo 27 del presente Reglamento o los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 de conformidad con el artículo 27, apartado 8, del presente Reglamento y, cuando no se hayan aplicado esas normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad, la descripción de las soluciones adoptadas para cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I, partes I y II, junto con una lista de otras especificaciones técnicas pertinentes aplicadas; en caso de normas armonizadas, especificaciones comunes o esquemas europeos de certificación de la ciberseguridad que se apliquen parcialmente, se especificarán en la documentación técnica las partes que se hayan aplicado;
6. informes de las pruebas realizadas para verificar la conformidad del producto con elementos digitales y de los procesos de gestión de las vulnerabilidades con los requisitos esenciales de ciberseguridad aplicables que se establecen en el anexo I, partes I y II;
7. una copia de la declaración UE de conformidad;
8. cuando proceda, la nomenclatura de materiales de los programas informáticos, previa solicitud motivada por parte de una autoridad de vigilancia del mercado, siempre que sea necesario para que dicha autoridad pueda comprobar el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en el anexo I.

▼B

ANEXO VIII

PROCEDIMIENTOS DE EVALUACIÓN DE LA CONFORMIDAD

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

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

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

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

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

4. Marcado de conformidad y declaración de conformidad

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

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

5. Representantes autorizados

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

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

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

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

▼B

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

La solicitud incluirá:

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

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

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

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

4. El organismo notificado:

4.1. examinará la documentación técnica y las pruebas para evaluar la adecuación del diseño técnico y del desarrollo del producto con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y la adecuación de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II;

4.2. comprobará que las muestras se han desarrollado o fabricado conforme a la documentación técnica, e identificará los elementos que se han diseñado y desarrollado con arreglo a las disposiciones aplicables de las normas armonizadas o especificaciones técnicas pertinentes, así como los elementos que se han diseñado y desarrollado sin aplicar las disposiciones pertinentes de dichas normas;

4.3. efectuará, o hará que se efectúen, los exámenes y pruebas oportunos para comprobar si, cuando el fabricante haya optado por aplicar las soluciones de las normas armonizadas o especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, su aplicación ha sido correcta;

4.4. efectuará, o hará que se efectúen, los exámenes y pruebas oportunas para comprobar si, en caso de que no se hayan aplicado las soluciones de las normas armonizadas o especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, las soluciones adoptadas por el fabricante cumplen los requisitos esenciales de ciberseguridad correspondientes;

4.5. acordará con el fabricante el lugar donde se realizarán los exámenes y las pruebas.

5. El organismo notificado elaborará un informe de evaluación que recoja las actividades realizadas de conformidad con el punto 4 y sus resultados. Sin perjuicio de sus obligaciones frente a las autoridades notificantes, el organismo notificado solo dará a conocer el contenido del informe, íntegramente o en parte, con el acuerdo del fabricante.

▼B

6. Si el tipo y los procesos de gestión de las vulnerabilidades cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, el organismo notificado expedirá al fabricante un certificado de examen de tipo UE. El certificado incluirá el nombre y la dirección del fabricante, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para la identificación del tipo aprobado y de los procesos de gestión de las vulnerabilidades. Se podrán adjuntar al certificado uno o varios anexos.

   El certificado y sus anexos contendrán toda la información pertinente que permita evaluar la conformidad de los productos con elementos digitales fabricados o desarrollados con el tipo examinado y los procesos de gestión de las vulnerabilidades, y permitir el control en servicio.

   En caso de que el tipo y los procesos de gestión de las vulnerabilidades no cumplan los requisitos esenciales de ciberseguridad aplicables establecidos en el anexo I, el organismo notificado se negará a expedir un certificado de examen de tipo UE e informará de ello al solicitante, explicando detalladamente su negativa.

7. El organismo notificado se mantendrá informado de las actualizaciones de la última tecnología conocida que indiquen que el tipo aprobado y los procesos de gestión de las vulnerabilidades ya no pueden cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I del presente Reglamento, y determinará si tales cambios requieren más investigaciones. En ese caso, el organismo notificado informará al fabricante en consecuencia.

   El fabricante informará al organismo notificado en posesión de la documentación técnica relativa al certificado de examen de tipo UE de todas las modificaciones del tipo aprobado y los procesos de gestión de las vulnerabilidades que puedan afectar a la conformidad con los requisitos esenciales de ciberseguridad establecidos en el anexo I o las condiciones de validez del certificado. Tales modificaciones requerirán una aprobación adicional en forma de suplemento al certificado original de examen de tipo UE.

8. El organismo notificado llevará a cabo auditorías periódicas para garantizar que los procesos de gestión de las vulnerabilidades establecidos en el anexo I, parte II, se aplican adecuadamente.

9. Cada organismo notificado informará a sus autoridades notificantes sobre los certificados de examen de tipo UE o cualquier añadido o añadidos a ellos que haya expedido o retirado, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de certificados o añadidos que hayan sido rechazados, suspendidos o restringidos de otro modo.

   Cada organismo notificado informará a los demás organismos notificados sobre los certificados de examen de tipo UE o los añadidos a estos certificados que haya rechazado, retirado, suspendido o restringido de otro modo, y, previa solicitud, sobre los certificados o sus añadidos que haya expedido.

   La Comisión, los Estados miembros y los demás organismos notificados podrán, previa solicitud, obtener una copia de los certificados de examen de tipo UE o cualquiera de sus suplementos. Previa solicitud, la Comisión y los Estados miembros podrán obtener una copia de la documentación técnica y los resultados de los exámenes efectuados por el organismo notificado. El organismo notificado conservará una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como del expediente técnico que incluya la documentación presentada por el fabricante hasta el final de la validez del certificado.

10. El fabricante conservará a disposición de las autoridades nacionales una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como la documentación técnica durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado.

11. El representante autorizado del fabricante podrá presentar la solicitud a que se refiere el punto 3 y cumplir las obligaciones contempladas en los puntos 7 y 10, siempre que las obligaciones pertinentes estén especificadas en su mandato.

▼B

Parte III Conformidad con el tipo basada en el control interno de la producción (basada en el módulo C)

1. La conformidad con el tipo basada en el control interno de la producción es la parte del procedimiento de evaluación de la conformidad según la cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 3 de la presente parte, y garantiza y declara que los productos con elementos digitales en cuestión son conformes con el tipo descrito en el certificado de examen de tipo UE y cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y que los fabricantes cumplen los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

2. Producción

El fabricante tomará todas las medidas necesarias para que la producción y su seguimiento garanticen la conformidad de los productos con elementos digitales fabricados con el tipo aprobado descrito en el certificado de examen de tipo UE y con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y garantizará que los fabricantes cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II.

3. Marcado de conformidad y declaración de conformidad

3.1. El fabricante colocará el marcado CE en los productos con elementos digitales que sean conformes al tipo descrito en el certificado de examen de tipo UE y satisfagan los requisitos aplicables establecidos en el instrumento legislativo.

3.2. El fabricante redactará una declaración de conformidad para un modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada. Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

4. Representante autorizado

Las obligaciones del fabricante establecidas en el punto 3 podrá cumplirlas su representante autorizado, en su nombre y bajo su responsabilidad, siempre que las obligaciones pertinentes estén especificadas en su mandato.

Parte IV Conformidad basada en el aseguramiento de calidad total (basada en el módulo H)

1. La conformidad basada en el aseguramiento de calidad total es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 5 de la presente parte, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos con elementos digitales (o las categorías de productos) en cuestión son conformes con los requisitos establecidos en el anexo I, parte I, y que los procesos de gestión de las vulnerabilidades establecidos por el fabricante cumplen los requisitos establecidos en el anexo I, parte II.

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

El fabricante aplicará un sistema de calidad aprobado, tal como se especifica en el punto 3, para el diseño, el desarrollo, la producción y la inspección y prueba finales de los productos con elementos digitales en cuestión y la gestión de las vulnerabilidades, lo mantendrá operativo a lo largo de todo el período de soporte y estará sujeto a la supervisión especificada en el punto 4.

▼B

3. Sistema de calidad

3.1. El fabricante presentará una solicitud de evaluación de su sistema de calidad ante el organismo notificado de su elección, para los productos con elementos digitales de que se trate.

La solicitud incluirá:

a) el nombre y la dirección del fabricante y, si la solicitud la presenta el representante autorizado, también el nombre y la dirección de este,

b) la documentación técnica para un modelo de cada categoría de productos con elementos digitales que se pretenda fabricar o desarrollar. La documentación técnica incluirá, cuando proceda, al menos los elementos establecidos en el anexo VII,

c) la documentación relativa al sistema de calidad, y

d) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de calidad garantizará la conformidad de los productos con elementos digitales con los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, y la conformidad de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos establecidos en el anexo I, parte II.

Todos los elementos, requisitos y disposiciones adoptados por el fabricante deberán reunirse de forma sistemática y ordenada en una documentación compuesta por políticas, procedimientos e instrucciones por escrito. Esta documentación del sistema de calidad permitirá una interpretación coherente de los programas, planes, manuales y registros de calidad.

En particular, incluirá una descripción adecuada de:

a) los objetivos de calidad, el organigrama y las responsabilidades y competencias del personal de gestión en lo que se refiere al diseño, el desarrollo, la calidad del producto y la gestión de las vulnerabilidades,

b) las especificaciones técnicas de diseño y desarrollo, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios que se utilizarán para asegurarse de que se cumplan los requisitos esenciales de ciberseguridad del anexo I, parte I, aplicables a los productos con elementos digitales,

c) las especificaciones de procedimiento, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios que se utilizarán para asegurarse de que se cumplan los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte II, aplicables al fabricante,

d) las técnicas de control y verificación del diseño y el desarrollo, los procesos y las medidas sistemáticas que se vayan a utilizar en el diseño y el desarrollo de los productos con elementos digitales por lo que se refiere a la categoría de productos de que se trate,

e) las correspondientes técnicas, procesos y actividades sistemáticas de producción, control de la calidad y aseguramiento de la calidad que se utilizarán,

f) los exámenes y las pruebas que se efectuarán antes, durante y después de la producción, y su frecuencia,

▼B

g) los expedientes de calidad, como los informes de inspección y datos de pruebas, los datos de calibrado y los informes sobre la cualificación del personal implicado,

h) los medios con los que se hace el seguimiento de la consecución del diseño y de la calidad exigidos de los productos y del funcionamiento eficaz del sistema de calidad.

3.3. El organismo notificado evaluará el sistema de calidad para determinar si cumple los requisitos a que se refiere el punto 3.2.

Dará por supuesta la conformidad con dichos requisitos de los elementos del sistema de calidad que cumplan las especificaciones correspondientes de la norma nacional que transponga la norma armonizada o la especificación técnica pertinente.

Además de experiencia en sistemas de gestión de la calidad, el equipo de auditoría tendrá, como mínimo, un miembro con experiencia como evaluador en el campo del producto pertinente y la tecnología del producto en cuestión, así como tendrá el conocimiento de los requisitos aplicables establecidos en el presente Reglamento. La auditoría incluirá una visita de evaluación a las instalaciones del fabricante, siempre que estas existan. El equipo de auditores revisará la documentación técnica mencionada en el punto 3.1, segundo guion, para comprobar si el fabricante es capaz de identificar los requisitos pertinentes establecidos en el presente Reglamento y de efectuar los exámenes necesarios a fin de garantizar que el producto con elementos digitales cumple dichos requisitos.

La decisión se notificará al fabricante o a su representante autorizado.

La notificación incluirá las conclusiones de la auditoría y la decisión de evaluación motivada.

3.4. El fabricante se comprometerá a cumplir las obligaciones que se deriven del sistema de calidad tal como se haya aprobado y a mantenerlo de forma que siga resultando adecuado y eficaz.

3.5. El fabricante mantendrá informado al organismo notificado que haya aprobado el sistema de calidad de cualquier adaptación prevista de dicho sistema.

El organismo notificado evaluará las adaptaciones propuestas y decidirá si el sistema de calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2, o si es necesaria una nueva evaluación.

El organismo notificado notificará su decisión al fabricante. La notificación incluirá las conclusiones del examen y la decisión de evaluación motivada.

4. Supervisión bajo la responsabilidad del organismo notificado

4.1. El objetivo de la supervisión es garantizar que el fabricante cumple debidamente las obligaciones que se derivan del sistema de calidad aprobado.

4.2. El fabricante permitirá la entrada del organismo notificado en los locales de diseño, desarrollo, producción, inspección, prueba y almacenamiento, a efectos de evaluación, y le proporcionará toda la información necesaria, en particular:

a) la documentación sobre el sistema de calidad,

b) los registros de calidad previstos en la parte del sistema de calidad dedicada al diseño, como los resultados de análisis, cálculos y pruebas,

c) los registros de calidad establecidos en la parte del sistema de calidad dedicada a la fabricación, tales como los informes de inspección, los datos sobre ensayos y calibración y los informes sobre la cualificación del personal afectado.

▼B

4.3. El organismo notificado realizará periódicamente auditorías para asegurarse de que el fabricante mantiene y aplica el sistema de calidad y proporcionará un informe de la auditoría al fabricante.

5. Marcado de conformidad y declaración de conformidad

5.1. El fabricante colocará el marcado CE y, bajo la responsabilidad del organismo notificado mencionado en el apartado 3.1, el número de identificación de este último en cada producto con elementos digitales que satisfaga los requisitos establecidos en el anexo I, parte I, del presente Reglamento.

5.2. El fabricante redactará una declaración de conformidad para cada modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada.

Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

6. El fabricante mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto con elementos digitales en el mercado o durante el período de soporte, si este fuese más prolongado:

a) la documentación técnica a que se refiere el punto 3.1;

b) la documentación relativa al sistema de calidad a que se refiere el punto 3.1;

c) las adaptaciones a que se refiere el punto 3.5 que hayan sido aprobadas;

d) las decisiones y los informes del organismo notificado a que se refieren los puntos 3.5 y 4.3.

7. Cada organismo notificado informará a sus autoridades notificantes sobre las aprobaciones de sistemas de calidad expedidas o retiradas, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de aprobaciones de sistemas de calidad que haya rechazado, suspendido o restringido de otro modo.

Cada organismo notificado informará a los demás organismos notificados sobre las aprobaciones de sistemas de calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido.

8. Representante autorizado

Las obligaciones del fabricante establecidas en los puntos 3.1, 3.5, 5 y 6 podrá cumplirlas, en su nombre y bajo su responsabilidad, su representante autorizado, siempre que las obligaciones pertinentes estén especificadas en el mandato.

En relación con el presente acto se ha formulado una declaración que se puede consultar en el DO C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.