REGLAMENTO DE CIBERRESILIENCIA

Gonzalo Iturmendi Morales

EL REGLAMENTO UE DE CIBERRESILIENCIA

GONZALO ITURMENDI MORALES.
BUFETE G. ITURMENDI Y ASOCIADOS SLP.
DIRECTOR DEL CENTRO DE ESTUDIOS DE AGERS.

ISBN: 978-84-09-74327-8

ÍNDICE

1. RELEVANCIA DE LA SEGURIDAD DE LOS PRODUCTOS CIBER

La amplitud del concepto legal de seguridad de los productos ciber o ciberseguridad lo encontramos en el artículo 2, punto 1, del Reglamento (UE) 2019/881: "todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas".

La seguridad general de los productos según el artículo 11 del Reglamento se refiere a la obligación de los productos con elementos digitales de cumplir con los requisitos de seguridad general establecidos en el Reglamento (UE) 2023/988, abarcando los riesgos no contemplados en otras legislaciones específicas de la Unión Europea.

El Reglamento establece normas para la comercialización de productos con elementos digitales, asegurando que estos productos cumplan con requisitos esenciales de ciberseguridad en su diseño, desarrollo y fabricación. Además, se imponen obligaciones a los operadores económicos para garantizar la ciberseguridad de estos productos durante su ciclo de vida.

El artículo 5 permite a los Estados miembros imponer requisitos adicionales de ciberseguridad para la contratación pública o el uso de productos con elementos digitales con fines específicos, como la seguridad nacional o la defensa, siempre que estos requisitos sean compatibles con las obligaciones establecidas en el Derecho de la Unión. Esto asegura que los productos utilizados en sectores críticos cumplan con estándares de ciberseguridad más estrictos.

El artículo 54 detalla el procedimiento a nivel nacional aplicable a los productos con elementos digitales que presentan un riesgo significativo de ciberseguridad. Las autoridades de vigilancia del mercado deben evaluar estos productos y, si no cumplen con los requisitos establecidos, solicitar medidas correctoras o retirar

los productos del mercado. Este artículo también establece la cooperación entre las autoridades de vigilancia del mercado y los operadores económicos para gestionar las vulnerabilidades y asegurar la conformidad de los productos.

El Reglamento incluye disposiciones específicas para la gestión de vulnerabilidades y la vigilancia del mercado, asegurando que los productos con elementos digitales sean evaluados y supervisados continuamente para mantener un alto nivel de ciberseguridad, estableciendo los requisitos horizontales de ciberseguridad para los productos con elementos digitales. Este Reglamento tiene como objetivo garantizar que los productos con elementos digitales comercializados en la Unión Europea cumplan con normas de ciberseguridad adecuadas para proteger a los consumidores y las organizaciones de los riesgos asociados a la ciberseguridad.

La norma europea abarca una amplia gama de productos, incluidos equipos y programas informáticos, y establece requisitos esenciales de ciberseguridad que los fabricantes deben cumplir. Estos requisitos incluyen la gestión de riesgos de ciberseguridad, la implementación de medidas de seguridad desde el diseño hasta la comercialización, y la provisión de actualizaciones de seguridad oportunas.

Además, el Reglamento establece procedimientos de evaluación de la conformidad para garantizar que los productos cumplan con los requisitos de ciberseguridad. Estos procedimientos incluyen evaluaciones iniciales, evaluaciones de vigilancia periódicas y evaluaciones de renovación de la certificación. Los organismos de evaluación de la conformidad deben ser independientes y cumplir con normas armonizadas para la acreditación.

La norma también aborda la relación con otros actos jurídicos de la Unión Europea, permitiendo la integración de la evaluación de riesgos de ciberseguridad en la documentación técnica exigida por otros Reglamentos. Esto facilita la conformidad de los productos con múltiples normativas de la UE

2. OBJETO DEL REGLAMENTO

El objeto del Reglamento, según su artículo 1, es establecer normas para la comercialización de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos. Además, el Reglamento define los requisitos esenciales de ciberseguridad para el diseño, desarrollo y fabricación de productos con elementos digitales, así como las obligaciones de los operadores económicos en relación con estos productos en lo que respecta a la ciberseguridad. También establece requisitos esenciales de ciberseguridad para los procesos de gestión de las vulnerabilidades que los fabricantes deben implementar para asegurar la ciberseguridad de los productos durante su uso previsto. Finalmente, el Reglamento incluye normas relativas a la vigilancia del mercado, supervisión y aplicación de los requisitos y normas mencionados.

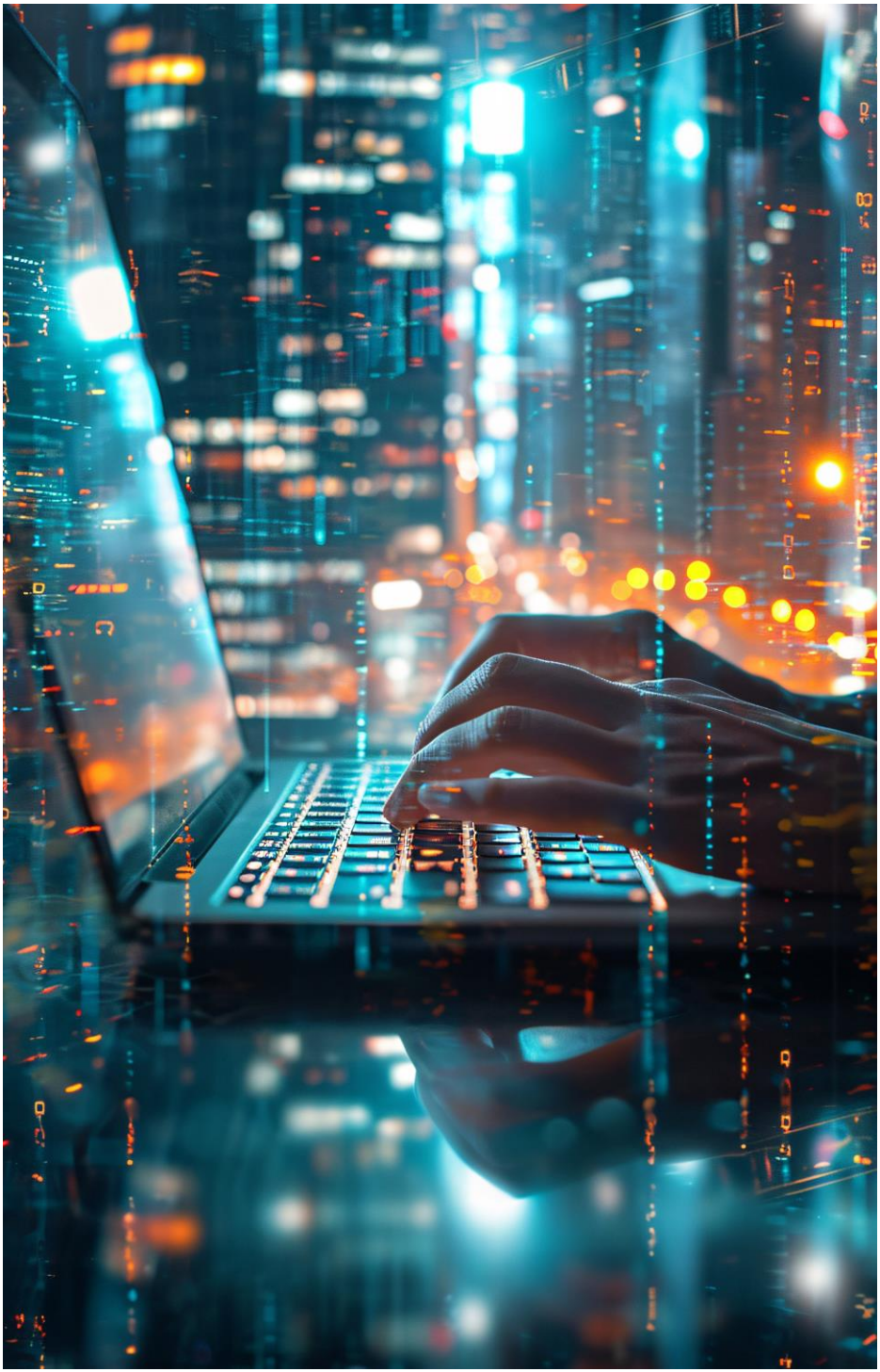
3. ÁMBITO DE APLICACIÓN

El Reglamento (UE) 2024/2847, de 23 de octubre de 2024, establece normas para la comercialización de productos con elementos digitales con el objetivo de garantizar la ciberseguridad de dichos productos. Este 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.

Sin embargo, el Reglamento no se aplica a ciertos productos con elementos digitales que están regulados por otros actos jurídicos de la Unión Europea. Estos incluyen el Reglamento (UE) 2017/745, el Reglamento (UE) 2017/746, el Reglamento (UE) 2019/2144, y los productos que hayan sido certificados de conformidad con el Reglamento (UE) 2018/1139. Además, no se aplica a los equipos que entran en el ámbito de aplicación de la Directiva 2014/90/UE del Parlamento Europeo y del Consejo.

El Reglamento también excluye de su ámbito de aplicación 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. Asimismo, 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.

Las obligaciones establecidas en esta norma 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.



4. PRINCIPIO DE LIBRE CIRCULACIÓN

El artículo 4 del Reglamento (UE) 2024/2847 establece los principios de libre circulación de productos con elementos digitales dentro de la Unión Europea. En primer lugar, se indica que los Estados miembros no impedirán la comercialización de productos con elementos digitales que sean conformes con el presente Reglamento. Esto significa que, siempre que los productos cumplan con los requisitos establecidos en el Reglamento, deben poder ser comercializados libremente en cualquier Estado miembro sin restricciones adicionales.

Además, el artículo permite que productos con elementos digitales que no sean conformes con el Reglamento puedan ser presentados o usados en ferias, exposiciones, demostraciones o actos similares, siempre y cuando se indique claramente que no son conformes y que no deben comercializarse hasta que lo sean. Esto facilita la innovación y el desarrollo de nuevos productos, permitiendo su exhibición y prueba antes de que cumplan con todos los requisitos reglamentarios.

Asimismo, el artículo permite la comercialización de programas informáticos inacabados que no sean conformes con el Reglamento, siempre que dichos programas solo se comercialicen durante un período de tiempo limitado y con fines de prueba, y que se indique claramente que no son conformes y que no se comercializarán con fines distintos de su prueba. Esto proporciona flexibilidad para el desarrollo y prueba de software antes de su lanzamiento definitivo.

Finalmente, el artículo especifica que el apartado anterior no se aplicará a los componentes de seguridad a que se refiere la legislación de armonización de la Unión distinta del presente Reglamento. Esto asegura que los componentes críticos de seguridad cumplan con los requisitos específicos establecidos en otras normativas de la Unión Europea.

5. REQUISITOS APLICABLES

El Reglamento (UE) 2024/2847 establece requisitos esenciales de ciberseguridad que los fabricantes deben cumplir para los productos con elementos digitales. Estos requisitos se dividen en dos partes: los requisitos relativos a las propiedades de los productos y los requisitos de gestión de las vulnerabilidades.

En la Parte I, los **requisitos de ciberseguridad relativos a las propiedades de los productos con elementos digitales** incluyen:

- Los productos deben diseñarse, desarrollarse y producirse de manera que garanticen un nivel adecuado de ciberseguridad basado en los riesgos existentes.

- Los productos deben comercializarse sin vulnerabilidades aprovechables conocidas y con una configuración segura por defecto. Además, deben garantizar que las vulnerabilidades puedan abordarse mediante actualizaciones de seguridad, incluidas las actualizaciones automáticas habilitadas como configuración por defecto.

- Los productos deben proteger contra el acceso no autorizado mediante mecanismos de control adecuados, proteger la confidencialidad e integridad de los datos personales o de otro tipo, y garantizar la disponibilidad de funciones esenciales y básicas, incluso tras un incidente.

- Los productos deben estar diseñados para limitar las superficies de ataque, reducir el impacto de un incidente y proporcionar información relacionada con la seguridad mediante el registro o seguimiento de la actividad interna pertinente.

- Los productos deben ofrecer a los usuarios la posibilidad de eliminar de manera segura y fácil todos los datos y parámetros de forma permanente.

En la Parte II, los **requisitos de gestión de las vulnerabilidades que los fabricantes deben cumplir** incluyen:

- Identificar y documentar las vulnerabilidades y los componentes presentes en el producto, incluyendo la elaboración de una nomenclatura de materiales de los programas informáticos.
- Abordar y subsanar las vulnerabilidades sin demora, mediante la provisión de actualizaciones de seguridad.
- Realizar exámenes y pruebas eficaces y periódicos de la seguridad del producto.
- Compartir y divulgar públicamente información sobre las vulnerabilidades solucionadas, incluyendo una descripción de las vulnerabilidades y la información que permita a los usuarios identificar el producto afectado.
- Implementar una política de divulgación coordinada de vulnerabilidades y facilitar el intercambio de información sobre posibles vulnerabilidades.
- Prever mecanismos para distribuir de manera segura las actualizaciones de los productos, garantizando que las vulnerabilidades se solucionen o se reduzcan de manera oportuna.
- Asegurarse de que las actualizaciones de seguridad se difundan sin demora y de forma gratuita, acompañadas de mensajes de aviso que proporcionen a los usuarios la información pertinente.

Estos requisitos son fundamentales para garantizar la ciberseguridad de los productos con elementos digitales durante todo su ciclo de vida, desde su diseño y desarrollo hasta su uso y mantenimiento.

6. PRODUCTOS CRÍTICOS CON ELEMENTOS DIGITALES

Según el Reglamento (UE) 2024/2847, los productos críticos con elementos digitales son aquellos cuya funcionalidad básica está relacionada con la ciberseguridad y desempeñan una función que conlleva un riesgo significativo de efectos adversos en términos de intensidad y capacidad para perturbar, controlar o dañar un gran número de otros productos con elementos digitales mediante manipulación directa. Estos productos se consideran dependencias críticas de las entidades esenciales mencionadas en el artículo 3, apartado 1, de la Directiva (UE) 2022/2555.

El Reglamento establece que las categorías de productos críticos con elementos digitales ya utilizan ampliamente diversas formas de certificación y están cubiertas por el esquema europeo de certificación de la ciberseguridad basado en criterios comunes establecidos en el Reglamento de Ejecución (UE) 2024/482 de la Comisión. Para garantizar una protección común adecuada de la ciberseguridad de estos productos en la Unión, puede ser adecuado y proporcionado someter dichas categorías de productos a una certificación europea obligatoria de la ciberseguridad cuando ya exista un esquema europeo de certificación pertinente que cubra esos productos y la Comisión haya llevado a cabo una evaluación del posible impacto en el mercado de la certificación obligatoria prevista.

El artículo 8 del Reglamento (UE) 2024/2847 establece que la Comisión está facultada para adoptar actos delegados para determinar qué productos con elementos digitales cuya funcionalidad básica es la de una categoría de productos establecida en el anexo IV del 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.

Las categorías de productos críticos con elementos digitales establecidas en el anexo IV del Reglamento incluyen dispositivos de equipos informáticos con cajas de seguridad, pasarelas de contadores inteligentes dentro de los sistemas de medición inteligente, y tarjetas inteligentes o dispositivos similares que incluyan elementos seguros.

7. SEGURIDAD DE PRODUCTOS

El artículo 11 del Reglamento (UE) 2024/2847 establece que la seguridad general de los productos se refiere a los aspectos y riesgos que no están contemplados en otros Reglamentos específicos de la Unión Europea. Este artículo indica que, a pesar de las disposiciones específicas de otros Reglamentos, los productos con elementos digitales deben cumplir con los requisitos de seguridad general establecidos en el Reglamento (UE) 2023/988.

En particular, el artículo 11 menciona que los productos con elementos digitales deben cumplir con los requisitos de seguridad general en lo que respecta a los riesgos o categorías de riesgos no contemplados en otros Reglamentos específicos. Esto implica que, además de cumplir con las normativas específicas aplicables a ciertos productos, estos deben garantizar un nivel elevado de protección de la salud y seguridad de las personas, asegurando que no presenten riesgos adicionales no cubiertos por otras legislaciones.

El artículo también establece que los productos con elementos digitales deben cumplir con los requisitos de seguridad general establecidos en el Reglamento (UE) 2023/988, que proporciona un marco general para la seguridad de los productos en la Unión Europea. Este Reglamento asegura que los productos sean seguros para los consumidores y usuarios, considerando todos los posibles riesgos asociados con su uso.

8. OBLIGACIONES DE LOS FABRICANTES

El Reglamento (UE) 2024/2847, conocido como el Reglamento de Ciberresiliencia, establece diversas obligaciones para los fabricantes de productos con elementos digitales. Estas obligaciones están diseñadas para garantizar la ciberseguridad de dichos productos y abarcan varios aspectos clave.

En primer lugar, los fabricantes deben asegurarse de que sus productos cumplan con los requisitos esenciales de ciberseguridad establecidos en el anexo I del Reglamento. Esto incluye tanto los requisitos para el diseño, desarrollo y fabricación de los productos como los requisitos para los procesos de gestión de vulnerabilidades.

Antes de introducir un producto en el mercado, los fabricantes deben llevar a cabo el procedimiento de evaluación de la conformidad especificado en el artículo 32 del Reglamento. Este procedimiento puede ser realizado por el propio fabricante o encargado a terceros en su nombre. Una vez demostrado que el producto cumple con los requisitos aplicables, los fabricantes deben elaborar una declaración UE de conformidad y colocar el marcado CE en el producto. .

Los fabricantes también tienen la obligación de conservar la documentación técnica y la declaración UE de conformidad durante un mínimo de diez años a partir de la introducción del producto en el mercado. Esta documentación debe estar disponible para las autoridades de vigilancia del mercado.

Además, los fabricantes deben asegurarse de que existen procedimientos para que la producción en serie del producto mantenga su conformidad con el Reglamento. Esto implica tener en cuenta los cambios en el diseño o las características del producto, así como los cambios en las normas armonizadas y otras especificaciones técnicas.

Es esencial que los productos con elementos digitales lleven un número de tipo, lote o serie, o cualquier otro elemento que permita su identificación. Si esto no es posible, la información requerida debe figurar en el embalaje o en un documento que acompañe al producto.

Los fabricantes deben indicar su nombre, nombre comercial registrado o marca registrada, así como su dirección postal y otros datos de contacto en el producto, su embalaje o en un documento que lo acompañe. Esta información debe ser clara, comprensible y legible.

También deben designar un punto de contacto único que permita a los usuarios comunicarse directamente con ellos, facilitando la notificación de vulnerabilidades del producto. Este punto de contacto debe ser fácilmente identificable por los usuarios.

Los productos con elementos digitales deben ir acompañados de la información y las instrucciones para el usuario especificadas en el anexo II del Reglamento. Estas instrucciones deben ser claras, comprensibles y legibles, y deben permitir la instalación, el funcionamiento y el uso seguros del producto.

Finalmente, los fabricantes deben adoptar medidas correctoras necesarias si descubren que un producto no es conforme con los requisitos esenciales de ciberseguridad. Esto puede incluir la retirada del producto del mercado o su recuperación. Además, deben informar a las autoridades de vigilancia del mercado y cooperar con ellas en cualquier medida destinada a eliminar los riesgos de ciberseguridad que presente el producto.

9. OBLIGACIONES ADICIONALES DE INFORMACIÓN DE LOS FABRICANTES

El Reglamento (UE) 2024/2847 establece diversas obligaciones de información para los fabricantes de productos con elementos digitales. Estas obligaciones están diseñadas para garantizar la ciberseguridad y la transparencia en la comercialización de dichos productos.

En primer lugar, los fabricantes deben notificar simultáneamente al CSIRT ("Computer Security Incident Response Team" o Equipo de Respuesta a Incidentes de Seguridad Informática designado como coordinador) y a la ENISA (Agencia de la Unión Europea para la Ciberseguridad) cualquier vulnerabilidad aprovechada activamente presente en el producto con elementos digitales de la que tengan conocimiento. Esta notificación debe realizarse a través de la plataforma única de notificación establecida en virtud del artículo 16 del Reglamento. La notificación debe incluir una alerta temprana de la vulnerabilidad, una descripción detallada de la misma, y un informe final con detalles sobre la actualización de seguridad o medidas correctoras disponibles para subsanar la vulnerabilidad.

Tengamos en cuenta que a Agencia de la Unión Europea para la Ciberseguridad desempeña un papel crucial en la mejora de la ciberseguridad en toda la Unión Europea, proporcionando asesoramiento y conocimientos especializados en cuestiones relacionadas con la ciberseguridad. Dicha Agencia actúa como un centro de conocimientos técnicos sobre ciberseguridad, asistiendo a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas de ciberseguridad. Además, fomenta la cooperación y la coordinación a nivel de la Unión entre los Estados miembros y las partes interesadas públicas y privadas en cuestiones de ciberseguridad. También

contribuye a la creación y mantenimiento de un marco europeo de certificación de la ciberseguridad, con el objetivo de aumentar la transparencia de la ciberseguridad de los productos, servicios y procesos de tecnologías de la información y comunicación (TIC) y reforzar la confianza en el mercado interior digital. La Agencia tiene la responsabilidad de apoyar la cooperación operativa entre los Estados miembros y las instituciones de la Unión, facilitando el intercambio de información y la gestión técnica de incidentes de ciberseguridad. ENISA organiza regularmente ejercicios de ciberseguridad a nivel de la Unión y elabora informes periódicos sobre la situación técnica de la ciberseguridad en la UE.

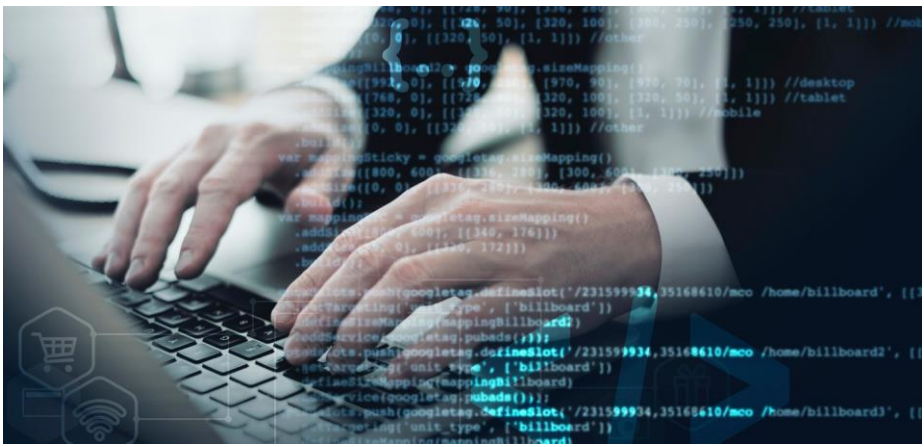
Por otro lado, los CSIRT (Equipos de Respuesta a Incidentes de Seguridad Informática)) son grupos de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información. Su función principal es gestionar y responder a incidentes de seguridad informática, proporcionando asistencia y soluciones para mitigar los efectos de dichos incidentes. Los CSIRT desempeñan un papel crucial en la protección de las redes y sistemas de información. Estos equipos están encargados de recibir notificaciones de incidentes de seguridad, analizar riesgos, supervisar incidentes a nivel nacional y difundir alertas sobre ellos. Además, los CSIRT colaboran con otros equipos nacionales e internacionales para garantizar una respuesta coordinada y eficaz ante los incidentes de ciberseguridad. Cada Estado miembro debe designar o establecer uno o varios CSIRT, asegurando que estos equipos dispongan de los recursos adecuados para llevar a cabo sus cometidos. Los CSIRT deben cumplir con ciertos requisitos, como garantizar la disponibilidad de sus canales de comunicación, la confidencialidad y fiabilidad de sus operaciones, y contar con personal suficiente y adecuadamente formado. Lógicamente los CSIRT deben cooperar entre sí y con otras partes interesadas pertinentes, tanto a nivel nacional como internacional, para mejorar la ciberseguridad y la gestión de riesgos. Esta cooperación incluye el intercambio de información sobre ciberamenazas, vulnerabilidades e incidentes, así como la asistencia mutua en la respuesta a incidentes transfronterizos.

Los fabricantes deben notificar cualquier incidente grave que repercuta en la seguridad de un producto con elementos digitales del que tengan conocimiento. Esta notificación también debe realizarse a través de la plataforma única de notificación y debe incluir una alerta temprana del incidente, una evaluación inicial del mismo, y un informe final con una descripción detallada del incidente y las medidas paliativas aplicadas.

Los fabricantes deben informar a los usuarios afectados del producto con elementos digitales sobre la vulnerabilidad o incidente y las medidas correctoras que los usuarios pueden adoptar para mitigar las repercusiones. Si el fabricante no informa en el plazo oportuno, los CSIRT designados como coordinadores pueden facilitar dicha información a los usuarios.

Finalmente, la Comisión adoptará actos delegados para especificar las condiciones de aplicación de los motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de notificaciones. También podrá especificar el formato y los procedimientos de las notificaciones mediante actos de ejecución.

Estas obligaciones de información son esenciales para mantener la seguridad y la confianza en los productos con elementos digitales, asegurando que los fabricantes actúen de manera proactiva y transparente ante cualquier riesgo de ciberseguridad.



10. OBLIGACIONES DE LOS IMPORTADORES

El Reglamento (UE) 2024/2847 establece requisitos horizontales de ciberseguridad para los productos con elementos digitales. Las obligaciones de los importadores según este Reglamento son diversas y están diseñadas para asegurar que los productos introducidos en el mercado cumplan con los requisitos esenciales de ciberseguridad.

En primer lugar, los importadores solo pueden introducir 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.

Antes de introducir un producto en el mercado, los importadores deben asegurarse de que el fabricante ha llevado a cabo los procedimientos de evaluación de la conformidad adecuados, ha redactado la documentación técnica, el producto lleva el marcado CE y va acompañado de la declaración UE de conformidad y de la información e instrucciones para el usuario especificadas en el anexo II. Además, deben verificar que el fabricante ha cumplido los requisitos establecidos en el artículo 13, apartados 15, 16 y 19.

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 Reglamento, no introducirá el producto en el mercado hasta que se haya puesto en conformidad. Además, si el producto presenta un riesgo de ciberseguridad significativo, el importador debe informar de ello al fabricante y a las autoridades de vigilancia del mercado.

Los importadores deben indicar su nombre, nombre comercial registrado o marca registrada, su dirección postal, dirección

de correo electrónico u otros datos de contacto digitales en el producto, en su embalaje o en un documento que lo acompañe. Esta información debe ser clara y comprensible para los usuarios finales y las autoridades de vigilancia del mercado.

Si los importadores saben o tienen motivos para creer que un producto que han introducido en el mercado no es conforme con el Reglamento, deben adoptar inmediatamente las medidas correctoras necesarias para garantizar que el producto se ponga en conformidad, o bien retirarlo del mercado o recuperarlo, cuando proceda. Además, deben informar a las autoridades de vigilancia del mercado de los Estados miembros en los que lo hayan comercializado y proporcionar detalles sobre la no conformidad y cualquier medida correctora adoptada.

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

Previa solicitud motivada de una autoridad de vigilancia del mercado, los importadores deben facilitar toda la información y documentación necesarias para demostrar la conformidad del producto 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. Deben cooperar con dicha autoridad en cualquier medida adoptada para eliminar los riesgos de ciberseguridad que presente el producto.

Finalmente, los importadores deben establecer canales de denuncia accesibles para que los usuarios puedan presentar reclamaciones, llevarunregistrodelasreclamaciones, delosproductosnoconformes y de las recuperaciones y retiradas de productos. Deben investigar las reclamaciones y realizar un seguimiento de la información

recibida relativa a incidentes que afecten a un producto que hayan comercializado, manteniendo informados de la investigación y el seguimiento realizados y de sus resultados al fabricante, a los distribuidores y, cuando proceda, a los representantes autorizados.

11. OBLIGACIONES DE LOS DISTRIBUIDORES

El Reglamento (UE) 2024/2847 establece diversas obligaciones para los distribuidores de productos con elementos digitales. Estas obligaciones están diseñadas para garantizar la conformidad y seguridad de los productos comercializados, así como para asegurar la cooperación con las autoridades de vigilancia del mercado.

En primer lugar, antes de comercializar un producto con elementos digitales, los distribuidores deben comprobar que el producto lleva el marcado CE y que el fabricante y el importador han cumplido con las obligaciones establecidas en el artículo 13, apartados 15, 16, 18, 19 y 20, y en el artículo 19, apartado 4. Además, deben asegurarse de que el fabricante ha facilitado todos los documentos necesarios al distribuidor

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 hasta que el producto o los procesos establecidos por el fabricante 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

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

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

Finalmente, 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.

12. CASOS EN QUE LAS OBLIGACIONES DE LOS FABRICANTES SON APLICABLES A LOS IMPORTADORES Y DISTRIBUIDORES

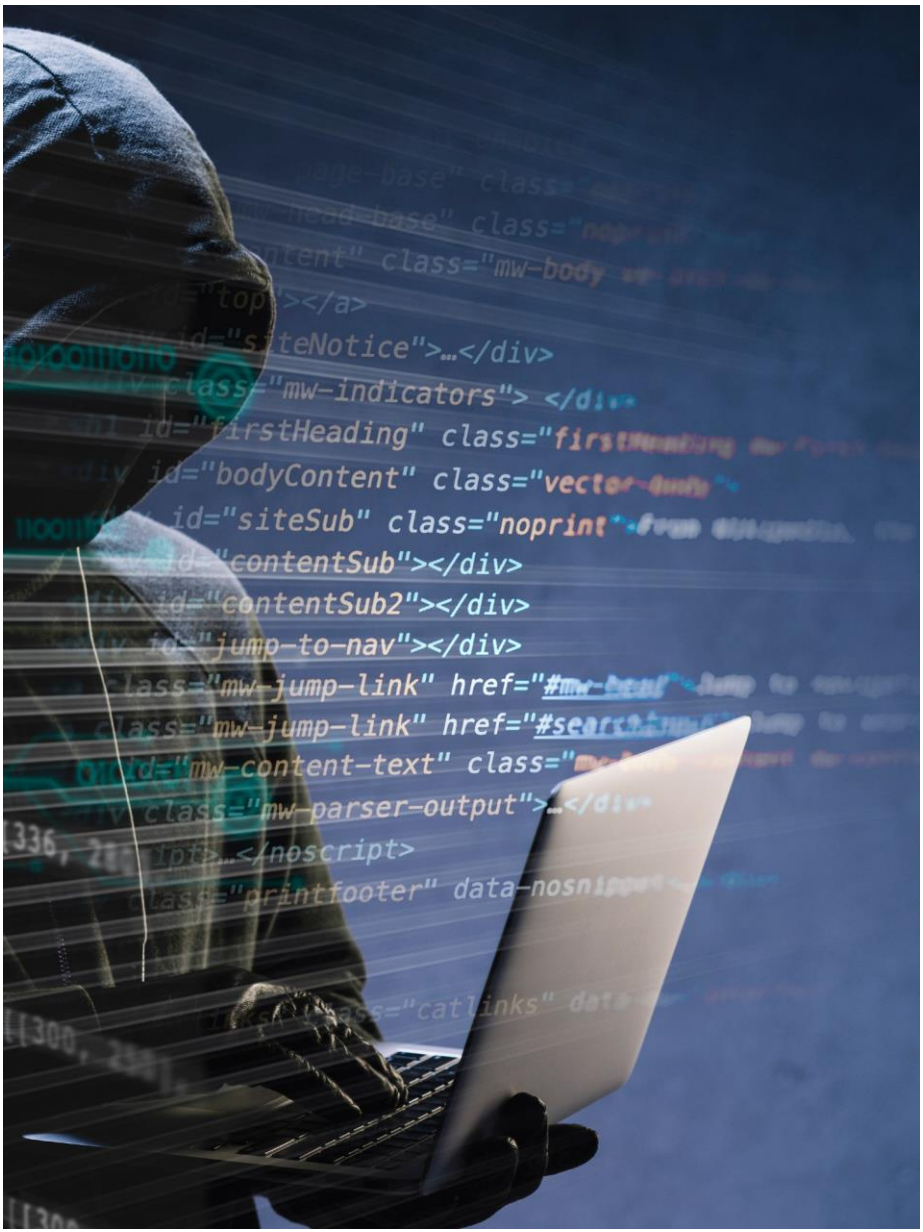
El Reglamento (UE) 2024/2847, conocido como el Reglamento de Ciberresiliencia, establece los requisitos horizontales de ciberseguridad para los productos con elementos digitales. En este contexto, los importadores y distribuidores pueden ser considerados fabricantes y, por lo tanto, estar sujetos a las obligaciones de los fabricantes en ciertos casos específicos.

Según el artículo 21 del Reglamento, los importadores o distribuidores serán considerados fabricantes y estarán sujetos a las obligaciones de los fabricantes cuando introduzcan en el mercado un producto con elementos digitales con su nombre o marca, o cuando lleven a cabo una modificación sustancial de un producto con elementos digitales que ya se haya introducido en el mercado.

Además, el artículo 22 del mismo Reglamento amplía esta consideración a cualquier persona física o jurídica, distinta del fabricante, importador o distribuidor, que lleve a cabo una modificación sustancial de un producto con elementos digitales y comercialice dicho producto. Esta persona deberá cumplir las obligaciones establecidas en los artículos 13 y 14 con respecto a la parte del producto afectada por la modificación sustancial o, si la modificación afecta a la ciberseguridad del producto en su conjunto, con respecto a la totalidad del producto.

En resumen, los importadores y distribuidores serán considerados fabricantes y deberán cumplir con las obligaciones correspondientes cuando introduzcan productos con elementos digitales en el mercado bajo su nombre o marca, o cuando realicen modificaciones

sustanciales que afecten la conformidad del producto con los requisitos de ciberseguridad establecidos en el Reglamento de Ciberresiliencia.



13. IDENTIFICACIÓN DE LOS OPERADORES ECONÓMICOS

Según el artículo 23, los operadores económicos son aquellos que participan en la cadena de suministro de productos con elemen tos digitales. Estos operadores tienen la obligación de facilitar información a las autoridades de vigilancia del mercado, incluyendo el nombre y la dirección de cualquier operador económico que les haya suministrado un producto con elementos digitales, así como el nombre y la dirección de cualquier operador económico al que hayan suministrado un producto con elementos digitales, cuando dispongan de ellos. Además, deben estar en condiciones de aportar esta información durante diez años a partir de que se les haya suministrado el producto y durante diez años a partir de que ellos hayan suministrado el producto El Reglamento establece requisitos horizontales de ciberseguridad para los productos con elementos digitales. En su artículo 23, se especifica cómo deben identificarse los operadores económicos.

Los operadores económicos deben proporcionar, previa solicitud, la siguiente información a las autoridades de vigilancia del mercado:

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

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

Además, los operadores económicos deben estar en condiciones de aportar esta información 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.

Este Reglamento asegura que la trazabilidad de los productos con elementos digitales se mantenga durante un período significativo, facilitando así la vigilancia del mercado y la adopción de medidas correctivas cuando sea necesario.

14. OBLIGACIONES DE LOS ADMINISTRADORES DE COMUNIDAD DE PROGRAMAS INFORMÁTICOS DE CÓDIGO ABIERTO

Se define «administrador de comunidad de programas informáticos de código abierto» como aquella 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.

Estas obligaciones están diseñadas para garantizar la ciberseguridad y la gestión eficaz de las vulnerabilidades en los productos con elementos digitales desarrollados dentro de estas comunidades.

En primer lugar, los administradores de comunidad de programas informáticos de código abierto deben establecer y documentar de manera verificable una política de ciberseguridad. Esta política tiene como objetivo fomentar el desarrollo de productos seguros y una gestión eficaz de las vulnerabilidades por parte de los desarrolladores. Además, la política debe promover la notificación voluntaria de vulnerabilidades y tener en cuenta la naturaleza específica del administrador de comunidad y las disposiciones jurídicas y organizativas a las que esté sujeto. La política debe incluir aspectos relacionados con la documentación de las vulnerabilidades, la respuesta a ellas y su subsanación, así como promover el intercambio de información sobre las vulnerabilidades descubiertas en la comunidad de código abierto

Asimismo, los administradores de comunidad de programas informáticos de código abierto deben cooperar con las autoridades de vigilancia del mercado, a petición de estas, para reducir los riesgos de ciberseguridad planteados por los productos con elementos digitales. Previa solicitud motivada de una autoridad de vigilancia del mercado, los administradores deben facilitar la documentación relacionada con la política de ciberseguridad en una lengua fácilmente comprensible para la autoridad, en papel o en formato electrónico

Además, las obligaciones establecidas en el artículo 14, apartado 1, del Reglamento 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, también se aplicarán a los administradores en la medida en que un incidente grave que repercuta en la seguridad de los productos afecte a las redes y sistemas de información proporcionados por los administradores para el desarrollo de los productos.

En resumen, los administradores de comunidad de programas informáticos de código abierto tienen la responsabilidad de establecer políticas de ciberseguridad, cooperar con las autoridades de vigilancia del mercado y cumplir con las obligaciones de notificación y gestión de incidentes graves, todo ello con el objetivo de garantizar la seguridad y resiliencia de los productos desarrollados en sus comunidades.

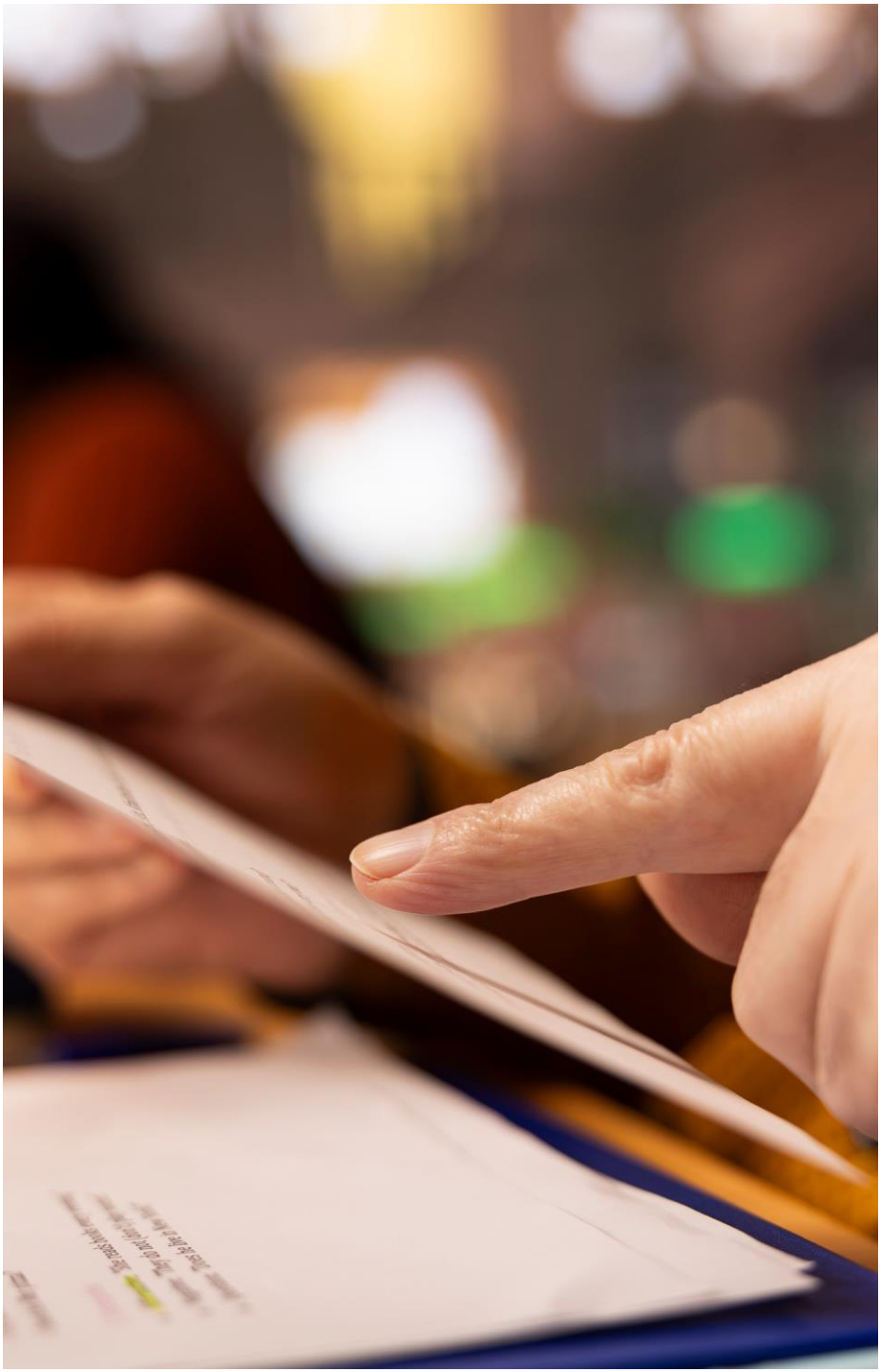
15. PRESUNCIÓN DE CONFORMIDAD

Se presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante son conformes con normas armonizadas cuando cumplan con los requisitos esenciales de ciberseguridad establecidos en el anexo I del Reglamento. Esta presunción de conformidad se basa en la publicación de las referencias de dichas normas armonizadas en el Diario Oficial de la Unión Europea.

La Comisión Europea, conforme al 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 establecidos en el anexo I del Reglamento de Ciberresiliencia. Al preparar estas solicitudes, la Comisión procurará tener en cuenta las normas europeas e internacionales en materia de ciberseguridad vigentes o en curso de desarrollo, con el fin de simplificar el desarrollo de las normas armonizadas.

Además, la Comisión está facultada para adoptar actos de ejecución que establezcan especificaciones comunes relativas a los requisitos técnicos que proporcionen un medio para cumplir los requisitos esenciales de ciberseguridad establecidos en el anexo I. Estos actos de ejecución se adoptarán cuando las normas armonizadas no hayan sido aceptadas, no se hayan entregado en el plazo establecido, no se ajusten a la solicitud, o no se haya publicado ninguna referencia a normas armonizadas en el Diario Oficial de la Unión Europea.

Por último, 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, o partes de estas, son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I.



16. REGLAS DE MARCADO DE LOS PRODUCTOS CON LAS SIGLAS CE

Se establecen las reglas y condiciones para la colocación del marcado CE en productos con elementos digitales en su artículo 30.

En primer lugar, el marcado CE debe colocarse de manera visible, legible e indeleble en el producto con elementos digitales. Si esto no es posible o no se justifica debido a la naturaleza del producto, el marcado CE se colocará en el embalaje y en la declaración UE de conformidad mencionada en el artículo 28 que acompañe al producto. En el caso de 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 en el sitio web que acompañe al producto. Los consumidores deben poder acceder de manera sencilla y directa al apartado pertinente del sitio web.

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

El marcado CE debe colocarse antes de que el producto con elementos digitales se introduzca en el mercado. Puede 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.

Asimismo, 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 elartículo 32. Dicho número de identificación delorganismo 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.

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.

Finalmente, 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 ("Grupo de Cooperación Administrativa" o Administrative Cooperation Group). El ADCO está compuesto por representantes de las autoridades de vigilancia del mercado designadas y, en su caso, por representantes de las oficinas de enlace únicas. La Comisión Europea apoya y fomenta la cooperación entre las autoridades de vigilancia del mercado a través de la Red de la Unión sobre Conformidad de los Productos, que incluye representantes de cada Estado miembro, un representante de cada oficina de enlace única, un experto nacional opcional, los presidentes de los ADCO y representantes de la Comisión. El ADCO también puede invitar a participar a expertos independientes y servir de enlace con otros ADCO, como el establecido con arreglo a la Directiva 2014/53/UE. Las autoridades de vigilancia del mercado, a través del ADCO, deben cooperar estrechamente y elaborar documentos de orientación para facilitar las actividades de vigilancia del mercado a nivel nacional, mediante el desarrollo de mejores prácticas e indicadores para comprobar eficazmente la conformidad de los productos con elementos digitales con el Reglamento de Ciberresiliencia.

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

17. VIGILANCIA DEL MERCADO Y CONTROL DE LOS PRODUCTOS CON ELEMENTOS DIGITALES EN EL MERCADO DE LA UNIÓN

La vigilancia del mercado y el control de los productos con elementos digitales en el mercado de la Unión Europea están regulados por el Reglamento (UE) 2024/2847, conocido como el Reglamento de Ciberresiliencia. Este Reglamento establece una serie de disposiciones para garantizar la ciberseguridad de los productos con elementos digitales y su conformidad con los requisitos establecidos.

En primer lugar, el Reglamento (UE) 2019/1020 es aplicable a los productos con elementos digitales que entran en el ámbito de aplicación del Reglamento de Ciberresiliencia. Cada Estado miembro debe designar una o varias autoridades de vigilancia del mercado para asegurar la aplicación efectiva del Reglamento. Estas autoridades pueden ser existentes o nuevas, y 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 del Reglamento de Ciberresiliencia.

Las autoridades de vigilancia del mercado deben cooperar con las autoridades nacionales de certificación de la ciberseguridad y con los CSIRT designados como coordinadores y la ENISA, especialmente en la supervisión de las obligaciones de información. Además, pueden solicitar asesoramiento técnico a un CSIRT o a la ENISA sobre cuestiones relacionadas con la aplicación y ejecución del Reglamento.

Los Estados miembros deben garantizar que las autoridades de vigilancia del mercado dispongan de recursos financieros y

técnicos adecuados, así como de personal con las capacidades necesarias en materia de ciberseguridad. La Comisión fomentará y facilitará el intercambio de experiencias entre las autoridades de vigilancia del mercado.

Las autoridades de vigilancia del mercado también tienen la responsabilidad de informar a los consumidores sobre dónde presentar reclamaciones que podrían indicar el incumplimiento del Reglamento y facilitar información sobre cómo acceder a mecanismos para la notificación de vulnerabilidades, incidentes y ciberamenazas. Además, deben cooperar con las partes interesadas pertinentes, incluidas las organizaciones científicas, de investigación y de consumidores.

En el caso de productos con elementos digitales que presenten un riesgo de ciberseguridad significativo, las autoridades de vigilancia del mercado deben realizar una evaluación del producto para verificar su cumplimiento con los requisitos del Reglamento. Si se constata que el producto no cumple los requisitos, se pedirá al operador económico que adopte las medidas correctoras oportunas o que retire el producto del mercado.

Además, el Reglamento establece un procedimiento de salvaguardia de la Unión para los productos con elementos digitales que presenten un riesgo de ciberseguridad significativo. La Comisión puede intervenir en circunstancias excepcionales para preservar el correcto funcionamiento del mercado interior y adoptar medidas correctoras o restrictivas a escala de la Unión.

Las autoridades de vigilancia del mercado también pueden llevar a cabo acciones de control simultáneas coordinadas, conocidas como “barridos”, para comprobar el cumplimiento o detectar infracciones del Reglamento. Estos barridos pueden incluir la inspección de productos adquiridos bajo una identidad encubierta.

En resumen, la vigilancia del mercado y el control de los productos con elementos digitales en el mercado de la Unión Europea según el Reglamento (UE) 2024/2847 implican una serie de medidas

y procedimientos destinados a garantizar la ciberseguridad y la conformidad de estos productos, con la cooperación de diversas autoridades y la participación activa de la Comisión y la ENISA.

Este manual constituye una obra de referencia imprescindible para comprender y aplicar el Reglamento (UE) de Ciberresiliencia, la nueva norma que redefine las exigencias de seguridad aplicables a los productos con elementos digitales en el mercado europeo. A través de un enfoque claro y sistemático, el autor desglosa los principios, requisitos y obligaciones que afectan a fabricantes, importadores, distribuidores y demás operadores económicos, proporcionando una visión práctica de la gestión de vulnerabilidades, el marcado CE y la vigilancia del mercado.

Dirigido a profesionales del derecho, responsables de cumplimiento normativo, fabricantes de tecnología y directivos, este libro permite anticipar riesgos, asegurar la conformidad regulatoria y convertir la ciberseguridad en una ventaja competitiva. Su lectura facilita no solo el cumplimiento de la norma, sino también la comprensión de un nuevo marco jurídico llamado a convertirse en pilar esencial de la confianza digital en la Unión Europea.

agers