2025/2392

1.12.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2392 DE LA COMISIÓN

de 28 de noviembre de 2025

sobre la descripción técnica de las categorías de productos importantes y críticos con elementos digitales con arreglo al Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el 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) ([1]), y en particular su artículo 7, apartado 4,

Considerando lo siguiente:

(1) El Reglamento (UE) 2024/2847 establece normas sobre ciberseguridad para los productos con elementos digitales. En particular, el anexo III de dicho Reglamento establece categorías de productos importantes con elementos digitales que, cuando se comercializan, están sujetos a procedimientos de evaluación de la conformidad más estrictos que los aplicables a otros productos con elementos digitales. El anexo IV del Reglamento (UE) 2024/2847 establece las categorías de productos críticos con elementos digitales a cuyos fabricantes se podría exigir la obtención de un certificado europeo de ciberseguridad en virtud de un esquema europeo de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([2]) o que estarían sujetos a una evaluación de la conformidad obligatoria por terceros cuando se comercialicen.

(2) De conformidad con el artículo 7, apartado 1, y el artículo 8, apartado 1, del Reglamento (UE) 2024/2847, la funcionalidad principal de un producto con elementos digitales determina si dicho producto con elementos digitales se ajusta a la descripción técnica de una categoría de productos importantes o críticos con elementos digitales y, por tanto, los procedimientos de evaluación de la conformidad aplicables.

(3) Al desarrollar un producto con elementos digitales, y para lograr el conjunto deseado de funcionalidades, los fabricantes suelen integrar en sus propios productos con elementos digitales otros componentes que también son productos con elementos digitales y que pueden cumplir la descripción técnica de una categoría de productos importantes o críticos. De conformidad con el Reglamento (UE) 2024/2847, un producto con elementos digitales está sujeto a los procedimientos de evaluación de la conformidad aplicables a los productos importantes o críticos con elementos digitales, si dicho producto en su conjunto es un producto importante o crítico, tal como se establece en los anexos III y IV de dicho Reglamento. Por ejemplo, la incorporación de un navegador integrado como componente de una aplicación de noticias para su uso en teléfonos inteligentes no hace que la aplicación esté sujeta al procedimiento de evaluación de la conformidad aplicable a los productos con elementos digitales que tengan como funcionalidad principal ser «navegadores independientes e integrados». No obstante, de conformidad con el Reglamento (UE) 2024/2847, el fabricante debe garantizar que el producto con elementos digitales en su conjunto cumpla los requisitos esenciales de ciberseguridad. Por lo tanto, el fabricante debe evaluar la seguridad del producto completo, teniendo en cuenta, según proceda, la seguridad de los componentes o funcionalidades integrados en él. Por ejemplo, para que el fabricante de una aplicación de noticias pueda demostrar que su producto con elementos digitales es conforme con el Reglamento (UE) 2024/2847, dicho fabricante debe demostrar que la aplicación de noticias en su conjunto cumple los requisitos aplicables, teniendo en cuenta, según proceda, la seguridad del navegador integrado en su aplicación.

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

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

(4) El hecho de que un producto con elementos digitales desempeñe funciones distintas o adicionales a las detalladas en las descripciones técnicas establecidas en el presente Reglamento no significa en sí mismo que el producto con elementos digitales no tenga la funcionalidad principal de una categoría de productos establecida en los anexos III y IV del Reglamento (UE) 2024/2847. Por ejemplo, los productos con elementos digitales que tienen como funcionalidad principal ser «sistemas operativos» suelen incluir programas informáticos que desempeñan funciones auxiliares no incluidas en la descripción técnica de esa categoría de productos, como calculadoras o editores gráficos simples. Los productos con elementos digitales a menudo también incorporan componentes que tienen la funcionalidad de otro producto importante o crítico con elementos digitales, como un sistema operativo que integre la funcionalidad de navegador o un enrutador que integre la funcionalidad de cortafuegos. Sin embargo, esto no significa en sí mismo que dichos productos con elementos digitales no tengan como funcionalidad principal ser «sistemas operativos» o «enrutadores, módems destinados a la conexión a internet y conmutadores», respectivamente.

(5) Por otra parte, un producto con elementos digitales que tenga la capacidad de realizar las funciones de una categoría de productos establecida en los anexos III y IV del Reglamento (UE) 2024/2847, pero cuya funcionalidad principal sea en sí misma diferente de la de tal categoría de productos, no debe considerarse que responde a la descripción técnica de dicha categoría de productos. Por ejemplo, un programa informático de orquestación, automatización y respuesta en materia de seguridad (SOAR, por sus siglas en inglés) suele tener la capacidad de realizar las funciones de productos con elementos digitales en la categoría de «sistemas de gestión de información y eventos de seguridad (SIEM, por sus siglas en inglés)», es decir, recopilar datos, analizarlos y presentarlos como información útil con fines de seguridad. Sin embargo, dado que su funcionalidad principal no es la de un SIEM, en general no debe considerarse que los programas informáticos SOAR responden a la descripción técnica de «sistemas de gestión de información y eventos de seguridad (SIEM)». Del mismo modo, un teléfono inteligente suele integrar componentes que desempeñan las funciones de varias categorías de productos establecidas en los anexos III y IV del Reglamento (UE) 2024/2847, como un sistema operativo o un gestor integrado de contraseñas. Sin embargo, dado que la funcionalidad principal de un teléfono inteligente no es la de ser un sistema operativo o un gestor de contraseñas, por lo general no debe considerarse que responde a la descripción técnica de dichas categorías de productos.

(6) De conformidad con el artículo 13, apartados 2 y 3, del Reglamento (UE) 2024/2847, los fabricantes de productos con elementos digitales deben aplicar los requisitos esenciales de ciberseguridad establecidos en el anexo I, parte I, del Reglamento (UE) 2024/2847 de manera proporcionada a los riesgos del producto con elementos digitales, basado en la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales, así como sus condiciones de uso, teniendo en cuenta el período de tiempo durante el que se prevé que el producto esté en uso. De conformidad con el artículo 13, apartados 2 y 3 de dicho Reglamento, y con independencia de que el producto con elementos digitales se considere un producto importante o crítico con elementos digitales, los fabricantes deben llevar a cabo una evaluación exhaustiva de los riesgos de ciberseguridad e indicar el modo en que se aplican los requisitos esenciales de ciberseguridad sobre la base de la evaluación de riesgos, incluidas sus pruebas y garantías. Cuando la funcionalidad principal de su producto con elementos digitales responda a la descripción técnica de un producto importante o crítico con elementos digitales, los fabricantes deben demostrar la conformidad con arreglo a los procedimientos de evaluación de la conformidad específicos establecidos en el artículo 32, apartados 2, 3, 4 y 5 del Reglamento (UE) 2024/2847.

(7) El presente Reglamento incluye ejemplos de productos con elementos digitales cuya funcionalidad principal responde a la descripción técnica de determinados productos importantes o críticos con elementos digitales. Estos ejemplos se ofrecen únicamente a título ilustrativo y no son una lista exhaustiva.

(8) A fin de proporcionar seguridad jurídica a los fabricantes, las categorías de productos con elementos digitales que son microprocesadores resistentes a manipulaciones, microcontroladores resistentes a manipulaciones y tarjetas inteligentes y dispositivos similares, incluidos los elementos seguros, deben distinguirse en función del nivel de resistencia frente a la posible explotación de los fallos o deficiencias para los que se han diseñado. El nivel AVA_VAN es un método ampliamente utilizado y normalizado para expresar ese nivel de resistencia. Los niveles AVA_VAN están establecidos en las normas de Criterios Comunes y en las Metodologías de Evaluación Comunes, que son de acceso público y sustentan los marcos de certificación existentes ampliamente adoptados en el mercado, como el Reglamento de Ejecución (UE) 2024/482 de la Comisión ([3]). El Reglamento de Ejecución (UE) 2024/482 establece un

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

esquema europeo de certificación de ciberseguridad que puede utilizarse para certificar un producto en función de su nivel de garantía. Sobre la base de las prácticas mundiales, el Reglamento de Ejecución (UE) 2024/482 prevé la posibilidad de expedir certificados basados en versiones anteriores de las normas hasta finales de 2027. Por tanto, en el contexto del Reglamento (UE) 2024/2847, es apropiado permitir la expresión de niveles AVA_VAN con referencia, bien a la última versión, bien a versiones anteriores de dichas normas.

(9) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité emitido en virtud del artículo 62, apartado 1, del Reglamento (UE) 2024/2847.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «criterios comunes»: los criterios comunes para la evaluación de la seguridad de las tecnologías de la información definidos en el artículo 2, apartado 1, del Reglamento de Ejecución (UE) 2024/482 o establecidos en las normas a que se refiere el artículo 3, apartado 2, letras a) y b), de dicho Reglamento de Ejecución;

2) «metodología común de evaluación»: metodología común para la evaluación de la seguridad de las tecnologías de la información tal como se define en el artículo 2, apartado 2, del Reglamento de Ejecución (UE) 2024/482 o establecidos en las normas a que se refiere el artículo 3, apartado 2, letras c) y d), de dicho Reglamento de Ejecución.

Artículo 2

1. La descripción técnica de las categorías de productos con elementos digitales de las clases I y II enumeradas en el anexo III del Reglamento (UE) 2024/2847 será la que figura en el anexo I del presente Reglamento.

2. La descripción técnica de las categorías de productos con elementos digitales enumeradas en el anexo IV del Reglamento (UE) 2024/2847 será la que figura en el anexo II del presente Reglamento.

Artículo 3

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

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

Hecho en Bruselas, el 28 de noviembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

PRODUCTOS IMPORTANTES CON ELEMENTOS DIGITALES

Clase I

Categoría de productos	Descripción técnica
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	Los sistemas de gestión de identidad son productos con elementos digitales que proporcionan mecanismos de autenticación o autorización y que también pueden proporcionar mecanismos para la gestión del ciclo de vida de las credenciales de identidad de personas físicas, personas jurídicas, dispositivos o sistemas, como el registro de identidad, la asignación de cuentas y permisos, el mantenimiento o la baja en el registro. Estos sistemas incluyen sistemas de gestión de acceso que controlan el acceso de personas físicas, personas jurídicas, dispositivos o sistemas a recursos digitales o lugares físicos. Un programa informático de gestión de accesos privilegiados es un sistema de gestión de acceso que controla y supervisa los derechos de acceso a los sistemas informáticos o a las tecnologías operativas y a la información sensible dentro de una organización, incluidos los sistemas que aplican políticas diferenciadas de control de acceso para los usuarios privilegiados. Esta categoría incluye, entre otras cosas, los lectores de autenticación y control de acceso, los lectores biométricos, los programas informáticos de inicio de sesión único, los programas informáticos de gestión de identidades federadas, los programas informáticos de contraseñas de un solo uso, los dispositivos de autenticación de equipos informáticos como los generadores de números de autenticación de transacciones (TAN, por sus siglas en inglés), los programas informáticos de autenticación y los programas informáticos de autenticación multifactor.
2. Navegadores independientes e integrados	Programas informáticos con elementos digitales que permiten a los usuarios finales acceder a contenidos y servicios web alojados en servidores conectados a redes como internet, renderizarlos e interactuar con ellos. Suelen incluir un motor de navegación web para interpretar y mostrar contenidos escritos en lenguaje de marcado (por ejemplo, HTML), apoyo para protocolos web (por ejemplo, HTTP o HTTPS), la capacidad de ejecutar *scripts* y gestionar las entradas de los usuarios, así como el almacenamiento de datos temporales o persistentes de sitios web (*cookies*). Esta categoría incluye, entre otras cosas, las aplicaciones independientes que cumplen las funciones de navegadores, los navegadores integrados destinados a la incorporación en otro sistema o aplicación, así como los navegadores con integración de agentes de IA.
3. Gestores de contraseñas	Productos con elementos digitales que almacenan contraseñas, localmente en un dispositivo o en un servidor remoto, incluyendo actividades como la generación de contraseñas, así como el uso compartido de contraseñas y la integración con aplicaciones locales o de terceros para el uso de contraseñas. Esta categoría incluye, entre otras cosas, los gestores de contraseñas locales, los gestores de contraseñas proporcionados como extensiones de navegadores, los gestores de contraseñas empresariales y los gestores de contraseñas basados en equipos informáticos.

Categoría de productos	Descripción técnica
4. Programas informáticos que buscan, eliminan o ponen en cuarentena programas informáticos maliciosos	Programas informáticos con elementos digitales, normalmente denominados antivirus o *antimalware*, que detectan o buscan programas informáticos maliciosos o código de dispositivos, o retiran o ponen en cuarentena dichos programas informáticos o código, con el fin de mantener la integridad, la confidencialidad o la disponibilidad de dichos dispositivos. En el contexto de esta categoría de productos, un programa informático malicioso es un programa informático que contiene funciones o capacidades maliciosas que pueden causar daño, directa o indirectamente, al usuario o al sistema informático, como virus, gusanos, programas de secuestro, programas espía y troyanos. Esta categoría incluye, entre otras cosas, los programas informáticos que detectan o buscan programas informáticos maliciosos en tiempo real o de forma manual, las herramientas de detección de *rootkits* y los discos de rescate cuya función principal sea buscar, eliminar o poner en cuarentena programas informáticos maliciosos.
5. Productos con elementos digitales que ejercen la función de red privada virtual (VPN, por sus siglas en inglés)	Productos con elementos digitales que establecen un túnel lógico cifrado construido a partir de los recursos del sistema de una red física o virtual. Esta categoría incluye, entre otras cosas, los clientes de redes privadas virtuales, los servidores de redes privadas virtuales y las pasarelas de redes privadas virtuales.
6. Sistemas de gestión de redes	Productos con elementos digitales que gestionan elementos de red conectados, como servidores, enrutadores, conmutadores, estaciones de trabajo, impresoras o dispositivos móviles, supervisándolos y controlando sus operaciones y configuraciones de red. Esta categoría incluye, entre otros, los sistemas de gestión de extremo a extremo y los sistemas específicos de gestión de la configuración, como los controladores para redes definidas por programas informáticos.
7. Sistemas de gestión de información de seguridad y eventos (SIEM, por sus siglas en inglés)	Productos con elementos digitales que recopilan datos de múltiples fuentes, analizan y correlacionan dichos datos y los presentan como información útil con fines relacionados con la seguridad, como la detección de amenazas e incidentes, el análisis forense o el cumplimiento.
8. Gestores de arranque	Programas informáticos con elementos digitales que gestionan el proceso de puesta en marcha inicial del sistema tras encenderlo o reiniciarlo, mediante la inicialización del equipo informático, la carga o transferencia del control al entorno del sistema operativo o a los recursos del sistema, y la selección de las opciones de arranque. Esta categoría incluye, entre otras cosas, el *firmware* UEFI y los cargadores, ya sean de una etapa o de varias etapas.
9. Infraestructuras de clave pública y programas informáticos de expedición de certificados digitales	Productos con elementos digitales utilizados como parte de una infraestructura de clave pública (PKI, por sus siglas en inglés) que gestionan la validación, creación, expedición, distribución, publicación de estado, renovación o revocación de certificados digitales, o la generación, almacenamiento, depósito, intercambio, destrucción o rotación de claves criptográficas asociadas a dichos certificados digitales. Esta categoría incluye, entre otras cosas, los sistemas de gestión de claves, los sistemas de gestión de certificados digitales, los respondedores del protocolo de estado de certificados en línea y las soluciones PKI integrales.

Categoría de productos	Descripción técnica
10. Interfaces físicas y virtuales de red	Las interfaces físicas de red son productos con elementos digitales que conectan directamente un dispositivo a una red a través de una interfaz de programación de aplicaciones (API, por sus siglas en inglés) proporcionada por los controladores de la interfaz, que normalmente funcionan en la capa de enlace de datos, y que incluyen adaptadores de equipos informáticos a los medios de transmisión con el *firmware* correspondiente, que normalmente funcionan en la capa física y de enlace de datos. Las interfaces virtuales de red son productos con elementos digitales que conectan directa o indirectamente un dispositivo a una red a través de una API que emula a la de los controladores de interfaces físicas de red, que suelen funcionar en la capa de enlace de datos. Esta categoría incluye, entre otras cosas, las tarjetas de interfaz de red por cable e inalámbricas, controladores y adaptadores, por ejemplo para Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee o Fieldbus, así como productos independientes puramente virtuales, como tarjetas de interfaces virtuales de red, interfaces de red para contenedores e interfaces VPN.
11. Sistemas operativos	Programas informáticos con elementos digitales que proporcionan una interfaz abstracta del equipo informático subyacente y controlan la ejecución de los programas informáticos, y que puedan prestar servicios como gestión y configuración de recursos informáticos, planificación, control de entradas y salidas, gestión de datos y suministro de una interfaz a través de la cual las aplicaciones interactúan con los recursos del sistema y los periféricos. Esta categoría incluye, entre otras cosas, los sistemas operativos en tiempo real, los sistemas operativos de uso general y los sistemas operativos para usos especiales.
12. Enrutadores, módems destinados a la conexión a internet y conmutadores	Los enrutadores son productos con elementos digitales que establecen y controlan el flujo de datos entre diferentes redes mediante la selección de itinerarios o rutas utilizando mecanismos y algoritmos de protocolo de enrutamiento, que suelen funcionar en la capa de red. Esta categoría incluye, entre otras cosas, los enrutadores por cable e inalámbricos, los enrutadores virtuales y los enrutadores con o sin módems.
	Los módems destinados a la conexión a internet son equipos informáticos con elementos digitales que utilizan técnicas digitales de modulación y desmodulación para convertir señales analógicas en señales digitales y viceversa para la comunicación basada en IP. Esta categoría incluye, entre otras cosas, los módems de fibra, los módems de línea de abonado digital (DSL), los módems de cable (DOCSIS), los módems satelitales y los módems celulares.
	Los conmutadores son productos con elementos digitales que proporcionan conectividad entre dispositivos de red a través de mecanismos de reenvío de paquetes y que cuentan con un plano de gestión, normalmente implantado en la capa de enlace de datos o en la capa de red. Esta categoría incluye, entre otras cosas, los conmutadores gestionados, los conmutadores inteligentes, los conmutadores multicapas, los conmutadores de seguridad virtuales, los conmutadores programables para redes definidas por programas informáticos y los puentes, como los puntos de acceso inalámbrico.

Categoría de productos	Descripción técnica
13. Microprocesadores con funcionalidades relacionadas con la seguridad	Productos con elementos digitales que son circuitos integrados que realizan funciones de procesamiento central dependiendo de memoria externa y periféricos, como microcódigo y otros *firmware* de bajo nivel. Además, ofrecen funcionalidades relacionadas con la seguridad, como el cifrado, la autenticación, el almacenamiento seguro de claves, la generación de números aleatorios, el entorno de ejecución fiable u otros mecanismos de protección basados en equipos informáticos, con el fin de proteger otros productos, redes o servicios más allá del propio microprocesador, como la cadena de arranque seguro, la virtualización o las interfaces de comunicación seguras.
14. Microcontroladores con funcionalidades relacionadas con la seguridad	Productos con elementos digitales que son circuitos integrados que realizan funciones de procesamiento central con memoria integrada que permite que el microcontrolador sea programable y, normalmente, también otros periféricos, como el microcódigo y otros *firmware* de bajo nivel. Además, ofrecen funcionalidades relacionadas con la seguridad, como el cifrado, la autenticación, el almacenamiento seguro de claves, la generación de números aleatorios, el entorno de ejecución fiable u otros mecanismos de protección basados en equipos informáticos, con el fin de proteger otros productos, redes o servicios más allá del propio microprocesador, como la cadena de arranque seguro, la virtualización o las interfaces de comunicación seguras.
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	Los circuitos integrados de aplicación específica (ASIC) con funcionalidades relacionadas con la seguridad son productos con elementos digitales que consisten en circuitos integrados, diseñados total o parcialmente a medida para realizar una función específica o ejecutar una aplicación específica, incluyendo el microcódigo y otros *firmware* de bajo nivel. Además, ofrecen funcionalidades relacionadas con la seguridad, como el cifrado, la autenticación, el almacenamiento seguro de claves, la generación de números aleatorios, el entorno de ejecución fiable u otros mecanismos de protección basados en equipos informáticos, con el fin de proteger otros productos, redes o servicios más allá del propio microprocesador, como la cadena de arranque seguro, la virtualización o las interfaces de comunicación seguras.
	Las matrices de puertas programables *in situ* (FPGA) con funcionalidades relacionadas con la seguridad son productos con elementos digitales que consisten en circuitos integrados caracterizados por una matriz de bloques lógicos configurables, diseñados para ser reprogramables tras su fabricación con el fin de realizar una función específica o ejecutar una aplicación específica, incluyendo el microcódigo y otros *firmware* de bajo nivel. Además, ofrecen funcionalidades relacionadas con la seguridad, como el cifrado, la autenticación, el almacenamiento seguro de claves, la generación de números aleatorios, el entorno de ejecución fiable u otros mecanismos de protección basados en equipos informáticos, con el fin de proteger otros productos, redes o servicios más allá del propio microprocesador, como la cadena de arranque seguro, la virtualización o las interfaces de comunicación seguras.
16. Asistentes virtuales de propósito general para hogares inteligentes	Productos con elementos digitales que se comunican mediante la internet pública, ya sea directamente o a través de otros equipos, que procesan solicitudes, tareas o preguntas basadas en instrucciones en lenguaje natural, por ejemplo mediante entradas de audio o por escrito, y que, sobre la base de esas solicitudes, tareas o preguntas, proporcionan acceso a otros servicios o controlan las funciones de los dispositivos conectados en entornos residenciales. Esta categoría incluye, entre otras cosas, los altavoces inteligentes con un asistente virtual integrado y los asistentes virtuales independientes que se ajustan a esta descripción.

Categoría de productos	Descripción técnica
17. Productos para hogares inteligentes con funciones de seguridad, como cerraduras, cámaras de seguridad, sistemas de vigilancia de bebés y sistemas de alarma inteligentes	Productos con elementos digitales que protegen la seguridad física de los consumidores en un entorno residencial y que pueden controlarse o gestionarse a distancia desde otros sistemas, así como los equipos y programas informáticos que controlan de forma centralizada dichos productos. Esta categoría incluye, entre otras cosas, los dispositivos inteligentes de bloqueo de puertas, los sistemas de vigilancia de bebés, los sistemas de alarma y las cámaras de seguridad en el hogar.
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 funcionalidades de seguimiento de localización	Los juguetes conectados a internet que tienen funciones sociales interactivas son productos con elementos digitales cubiertos por la Directiva 2009/48/CE, que se comunican con la internet pública, ya sea directamente o a través de cualquier otro equipo, y que tienen tecnologías integradas que permiten la comunicación entrante y saliente, como teclado, micrófono, altavoz o cámara.
	Los juguetes conectados a internet que tienen funciones de seguimiento de la ubicación son productos con elementos digitales cubiertos por la Directiva 2009/48/CE, que se comunican en la internet pública, ya sea directamente o a través de cualquier otro equipo, y que cuentan con tecnologías que permiten rastrear o inferir la ubicación geográfica del juguete o de su usuario. Cuando el juguete se limite a detectar la proximidad del usuario o de otros juguetes utilizando tecnologías de detección, no se considerará que el juguete tiene funciones de seguimiento de la ubicación.
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 ([2]) ni el Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo ([3]), o productos ponibles personales destinados a ser utilizados por y para niños.	Los productos ponibles personales destinados a ser utilizados o colocados en el cuerpo humano con fines de seguimiento médico son productos con elementos digitales que se llevan en el cuerpo directamente o a través de prendas o accesorios y que pueden, de forma periódica o continua, captar y procesar información, incluidos los parámetros corporales, pertinentes para la salud del usuario, excluidos los productos comprendidos en el ámbito de aplicación del Reglamento (UE) 2017/745 o del Reglamento (UE) 2017/746. Esta categoría incluye, entre otras cosas, los monitores de actividad, los relojes inteligentes, la ropa inteligente y las prendas deportivas que respondan a esta descripción.
	Los productos ponibles personales destinados a ser utilizados por niños y para niños son productos con elementos digitales que pueden utilizarse o colocarse en el cuerpo, directamente o a través de prendas o accesorios, por personas menores de 14 años. Esta categoría incluye, entre otras cosas, los dispositivos portátiles de seguridad para niños.

([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, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico *in vitro* y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Clase II

Categoría de productos	Descripción técnica
1. Hipervisores y sistemas de ejecución de contenedores que permiten la ejecución virtualizada de sistemas operativos y entornos similares	Los hipervisores son programas informáticos con elementos digitales que abstraen o asignan recursos informáticos y permiten la ejecución, gestión y orquestación de máquinas virtuales que están separadas lógicamente entre sí o del equipo informático físico. Los hipervisores pueden funcionar directamente en equipos informáticos (servidor dedicado), como añadidura a un sistema operativo o dentro de otra máquina virtual (virtualización anidada). En el contexto de esta categoría de productos, una máquina virtual es una separación lógica definida por la parte programática de un entorno informático, que incluye un conjunto virtualizado de recursos de equipos informáticos (por ejemplo, CPU, memoria, almacenamiento, interfaces de red) y normalmente alberga su propio sistema operativo. Esta categoría incluye, entre otras cosas, los hipervisores de tipo 1 (servidores dedicados), los hipervisores del tipo 2 (alojados en un sistema operativo) y los hipervisores híbridos.
	Los sistemas de ejecución de contenedores son programas informáticos con elementos digitales que gestionan la ejecución y el ciclo de vida de los contenedores que funcionan en un único sistema operativo de alojamiento como procesos aislados, asignan recursos y permiten la gestión y la orquestación de contenedores individuales. En el contexto de esta categoría de productos, un contenedor es un entorno de ejecución basado en programas informáticos que contiene uno o más componentes y sus dependencias en un único paquete, lo que le permite funcionar de manera independiente y coherente.
2. Cortafuegos y sistemas de detección y prevención de intrusiones	Los cortafuegos son productos con elementos digitales que protegen una red o sistema conectados del acceso no autorizado mediante el seguimiento y la restricción del tráfico de comunicaciones de datos hacia y desde dicha red. Esta categoría incluye, entre otras cosas, los cortafuegos de redes y los cortafuegos de aplicaciones, como los cortafuegos de aplicaciones web o los filtros y las pasarelas de filtrado de correo no deseado.
	Los sistemas de detección de intrusiones son productos con elementos digitales que supervisan el tráfico una vez que ha entrado en el entorno de la red en busca de actividades sospechosas y detectan o perciben que se ha intentado, se está produciendo o se ha producido una intrusión en una red o sistema conectados. Esta categoría incluye, entre otras cosas, los sistemas de detección de intrusiones en redes y los sistemas de detección de intrusiones en ordenadores centrales.
	Los sistemas de prevención de intrusiones son productos con elementos digitales compuestos por un sistema de detección de intrusiones que responde activamente a una intrusión en una red o sistema conectados. Esta categoría incluye, entre otras cosas, los sistemas de prevención de intrusiones en redes y los sistemas de prevención de intrusiones en ordenadores centrales.

Categoría de productos	Descripción técnica
3. Microprocesadores resistentes a las manipulaciones	Los productos con elementos digitales que sean microprocesadores con funcionalidades relacionadas con la seguridad a los que se refiere el cuadro «Clase I», punto 13, del presente anexo, incluidas las pruebas de manipulación, resistencia o respuesta, y que además estén diseñados para proporcionar protección de nivel AVA_VAN 2 o 3, tal como se establece en los criterios comunes y la metodología común de evaluación.
4. Microcontroladores resistentes a las manipulaciones.	Productos con elementos digitales que sean microcontroladores con funcionalidades relacionadas con la seguridad a los que se refiere el cuadro «Clase I», punto 14, del presente anexo, incluidas las pruebas de manipulación, resistencia o respuesta, y que además estén diseñados para proporcionar protección de nivel AVA_VAN 2 o 3, tal como se establece en los criterios comunes y la metodología común de evaluación.

ANEXO II

PRODUCTOS CRÍTICOS CON ELEMENTOS DIGITALES

Categoría de productos	Descripción técnica
1. Dispositivos de equipos informáticos con cajas de seguridad	Equipos informáticos con elementos digitales que almacenan, procesan o gestionan de forma segura datos sensibles o realizan operaciones criptográficas, y que consisten en múltiples componentes discretos, que incorporan una carcasa o envolvente física del equipo informático que proporciona pruebas de manipulación, resistencia o respuesta como contramedidas frente a ataques físicos. Esta categoría incluye, entre otras cosas, los terminales físicos de pago, los módulos de seguridad de los equipos informáticos que generan y gestionan elementos criptográficos y los tacógrafos que respondan a la descripción anterior.
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	Las pasarelas de contadores inteligentes son productos con elementos digitales que controlan la comunicación entre los componentes de los sistemas de medición inteligente o conectados a ellos, tal como se definen en el artículo 2, punto 23, de la Directiva (UE) 2019/944, y terceros autorizados, como los proveedores de servicios públicos. Las pasarelas de contadores inteligentes recogen, procesan y almacenan datos de medición o personales, protegen los flujos de datos e información mediante el apoyo a necesidades criptográficas específicas, como el cifrado y el descifrado de datos, incorporan funcionalidades de cortafuegos y proporcionan los medios para controlar otros dispositivos. Esta categoría incluye, entre otras cosas, las pasarelas de contadores inteligentes relacionadas con los sistemas de medición inteligente que miden la electricidad, tal como se definen en el artículo 2, apartado 23, de la Directiva (UE) 2019/944. También puede incluir pasarelas de contadores inteligentes utilizadas en otros sistemas de medición inteligente que midan el consumo de otras fuentes de energía, como el gas o la calefacción, siempre que la pasarela responda a esta descripción.
3. Tarjetas inteligentes o dispositivos similares, que incluyan elementos seguros	Los elementos seguros son microcontroladores o microprocesadores con funcionalidades relacionadas con la seguridad, incluidas las pruebas de manipulación, resistencia o respuesta. Normalmente almacenan, procesan o gestionan operaciones criptográficas o datos sensibles, como las credenciales de identidad o las credenciales de pago. Los elementos seguros están diseñados para proporcionar protección al menos a AVA_VAN.4, tal como se establece en los criterios comunes o en la metodología común de evaluación. Pueden ser semiconductores discretos o integrarse en sistemas en un chip (SoC, por sus siglas en inglés). Los elementos seguros pueden incorporar un entorno de aplicación o un sistema operativo, y pueden incluir una o más aplicaciones. Esta categoría incluye, entre otras cosas, los módulos de plataforma segura (TPM, por sus siglas en inglés) y la tarjeta de circuito integrado universal (UICC, por sus siglas en inglés).
	Las tarjetas inteligentes o dispositivos similares son elementos seguros integrados en un material portador, como plástico o madera, en forma de tarjeta, o elementos seguros integrados en materiales portadores que adoptan otras formas. Esta categoría incluye, entre otras cosas, los documentos de identidad y de viaje, las tarjetas de firma electrónica cualificada, las UICC sustituibles, las tarjetas de pago físicas, las tarjetas de acceso físico, las tarjetas de tacógrafo digital o las pulseras digitales con elementos de pago seguro integrados.

([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, ELI: http://data.europa.eu/eli/dir/2019/944/oj).