ANTEPROYECTO DE REAL DECRETO, DE X DE X, POR EL QUE SE DESIGNA A LA AUTORIDAD NOTIFICANTE Y A LA AUTORIDAD DE VIGILANCIA DEL MERCADO PARA LOS PRODUCTOS CON ELEMENTOS DIGITALES, EN CUMPLIMIENTO DEL *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.° 168/2013 Y EL REGLAMENTO (UE) 2019/1020 Y LA DIRECTIVA (UE) 2020/1828 (REGLAMENTO DE CIBERRESILIENCIA)*.

PREÁMBULO

I

La Unión Europea ha establecido un marco jurídico uniforme de requisitos horizontales de ciberseguridad para los productos con elementos digitales mediante 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 (en adelante, Reglamento de Ciberresiliencia).

La finalidad de este Reglamento de Ciberresiliencia es reforzar la ciberresiliencia del mercado interior, garantizar un nivel elevado y coherente de seguridad a lo largo del ciclo de vida de los productos con elementos digitales y ofrecer seguridad jurídica a los operadores económicos y a los usuarios.

El Reglamento de Ciberresiliencia se articula en torno a requisitos esenciales de ciberseguridad y a obligaciones de diseño, desarrollo, fabricación, mantenimiento, gestión de vulnerabilidades y actualizaciones durante un período de soporte adecuado. Asimismo, complementa la Directiva (UE) 2022/2555 (NIS 2) en cuanto al aumento de la resiliencia de servicios y cadenas de suministro en la Unión.

Conforme a su artículo 52.1, el Reglamento (UE) 2019/1020, relativo a la vigilancia del mercado y la conformidad de los productos, es aplicable a los productos con elementos digitales comprendidos en el ámbito del Reglamento de Ciberresiliencia. En consecuencia, los Estados miembros deben designar una o más autoridades de vigilancia de mercado para la efectiva implementación del Reglamento de Ciberresiliencia, sin perjuicio de las restantes obligaciones de cooperación y de intercambio de información previstas en el Derecho de la Unión.

En el ordenamiento español, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales ya viene ejerciendo funciones de autoridad de vigilancia del mercado en ámbitos afines, como el Reglamento Delegado (UE) 2022/30 de la Comisión, que complementa la Directiva 2014/53/UE (RED) en materia de requisitos de ciberseguridad aplicables a determinados equipos radioeléctricos, lo que constituye un antecedente operativo directo y aconseja su designación como autoridad de vigilancia del mercado a efectos del Reglamento de Ciberresiliencia.

Por su parte, el Centro Criptológico Nacional ostenta la condición de Autoridad Nacional de Certificación de la Ciberseguridad al amparo del Reglamento (UE) 2019/881, acumulando experiencia que resulta idónea para asumir las funciones de autoridad notificante previstas en el Reglamento de Ciberresiliencia. El presente real decreto se entiende sin perjuicio de las competencias que el resto del ordenamiento jurídico atribuye al Centro Criptológico Nacional.

Asimismo, la S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE) ostenta la condición de Centro de Coordinación Nacional (NCC-ES) en España del Centro Europeo de Competencia en Ciberseguridad (ECCC) y dispone de capacidades técnico-científicas y de laboratorio, así como de probada trayectoria de apoyo al sector privado y a la ciudadanía, que justifican su designación como laboratorio técnico de apoyo preferente de la autoridad de vigilancia del mercado en materia de productos con elementos digitales, sin atribución de potestades públicas ni facultades decisorias.

El presente real decreto tiene por objeto designar la Autoridad de Vigilancia del Mercado y la Autoridad Notificante a efectos del Reglamento de Ciberresiliencia, establecer su marco básico de cooperación y coordinación con las demás autoridades competentes, y asegurar la adecuada articulación con el régimen general de vigilancia del mercado del Reglamento (UE) 2019/1020. A tal fin, se prevé la utilización de los sistemas de información de la Unión (entre ellos, NANDO e ICSMS), la coordinación con la oficina de enlace única regulada en el Reglamento (UE) 2019/1020 y mecanismos estables de cooperación interadministrativa que eviten solapamientos y garanticen la coherencia en la aplicación del Reglamento de Ciberresiliencia.

Asimismo, a los solos efectos de facilitar la comprensión y el cumplimiento del Reglamento por parte de las microempresas y pymes, este real decreto prevé la posibilidad de que la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en coordinación con INCIBE, adopte medidas de apoyo de carácter informativo y de sensibilización, conforme al artículo 33 del Reglamento de Ciberresiliencia.

Estas actuaciones se encuadran en las funciones de planificación, coordinación, desarrollo e impulso de políticas de ciberseguridad en el entorno privado atribuidas al Departamento, sin creación de nuevas obligaciones ni de derechos para los operadores económicos ni compromisos de gasto adicionales

II

El presente real decreto se ajusta a los principios de buena regulación a los que se refiere el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en particular a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. Cumple con los principios de necesidad y eficacia puesto que está justificado en las razones de interés general descritas en los párrafos precedentes y constituye el instrumento más adecuado para garantizar la consecución de las metas propuestas.

En cuanto al cumplimiento del principio de proporcionalidad, esta norma contiene la regulación imprescindible para atender las necesidades identificadas, de modo que para lograr los objetivos fijados no existen otras medidas menos restrictivas de derechos o que impongan menos obligaciones a los destinatarios. Es decir, las posibles limitaciones de derechos y obligaciones impuestas por la norma son proporcionales a los fines perseguidos y se justifican en el carácter obligatorio de dar cumplimiento a lo establecido por el Reglamento de Ciberresiliencia.

Al mismo tiempo, la necesaria adaptación de la normativa nacional aplicable a los productos con elementos digitales a las normas de la Unión Europea redunda en una mayor seguridad jurídica, dotando de coherencia y estabilidad al marco normativo en esta materia. Con este fin, el real decreto incorpora medidas organizativas que aprovechan estructuras ya existentes, evitando cargas administrativas adicionales, y refuerza la cooperación con las autoridades y organismos nacionales competentes, incluyendo la colaboración técnica con INCIBE como laboratorio de apoyo preferente.

Este real decreto no introduce ni establece trámites adicionales o distintos a los contemplados en la Ley 39/2015, de 1 de octubre.

Se dicta a propuesta del Ministro para la Transformación Digital y de la Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día XX de X de XXXX.

DISPONGO

Artículo 1. Objeto

Este real decreto tiene por objeto designar a la Autoridad de Vigilancia del Mercado y la Autoridad Notificante a efectos del 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 (en adelante, Reglamento de Ciberresiliencia), así como articular su marco básico de cooperación y coordinación para la aplicación del Reglamento de Ciberresiliencia en España, sin perjuicio de la aplicación del Reglamento (UE) 2019/1020 en materia de vigilancia del mercado de los productos con elementos digitales comprendidos en el ámbito del Reglamento de Ciberresiliencia.

Artículo 2. Definiciones

A los efectos de este real decreto, serán de aplicación las definiciones del artículo 3 del Reglamento de Ciberresiliencia. En lo no previsto, se aplicarán las definiciones del Reglamento (UE) 2019/1020 y las que se establezcan en los actos delegados y de ejecución adoptados conforme al Reglamento de Ciberresiliencia.

Artículo 3. Ámbito de aplicación

1. Este real decreto será de aplicación a los productos con elementos digitales incluidos en el ámbito de aplicación del Reglamento de Ciberresiliencia que se introduzcan o se pongan a disposición en el mercado en España.
2. Quedan excluidos los productos y equipos recogidos en los supuestos de no aplicación previstos en el artículo 2 del Reglamento de Ciberresiliencia y, en su caso, los establecidos en otros actos jurídicos de la Unión que resulten de aplicación preferente.
3. Quedan excluidos los productos y equipos que el Reglamento de Ciberresiliencia excluye de su ámbito de aplicación, de conformidad con su artículo 2, así como, en su caso, aquellos respecto de los cuales otros actos jurídicos de la Unión establezcan un régimen de aplicación preferente.

Artículo 4. Obligaciones de los operadores económicos

Los operadores económicos a los que se refiere el Reglamento de Ciberresiliencia cumplirán las obligaciones previstas en el capítulo II de dicho Reglamento, incluidas, en su caso, las relativas a la gestión de vulnerabilidades y a las obligaciones de información. Todo ello sin perjuicio de las responsabilidades que les correspondan conforme al Derecho de la Unión y nacional aplicable y, cuando proceda, del cumplimiento de los actos de armonización de la Unión aplicables al producto, en particular del Reglamento (UE) 2023/1230 sobre maquinaria.

Artículo 5. Presunción y evaluación de la conformidad

1. La presunción de conformidad con los requisitos esenciales del anexo I del Reglamento de Ciberresiliencia se regirá por lo especificado en dicho Reglamento, en particular:
    a) La aplicación de normas armonizadas o especificaciones comunes en los términos previstos en dicho Reglamento.
    b) La expedición de una declaración UE de conformidad o de un certificado europeo de ciberseguridad al amparo de un esquema europeo de certificación de la ciberseguridad adoptado conforme al Reglamento (UE) 2019/881, en la medida en que la declaración o el certificado cubran los requisitos esenciales, de acuerdo con el artículo 27.8.
2. De acuerdo con el artículo 27.9 del Reglamento de Ciberresiliencia, la Comisión podrá especificar, mediante actos delegados, qué esquemas europeos de certificación sirven para demostrar la conformidad con los requisitos esenciales o partes de éstos. La expedición de un certificado con nivel de garantía al menos “sustancial” en el marco de dichos esquemas eliminará la obligación del fabricante de someterse a evaluación por tercera parte para los requisitos correspondientes, según lo previsto en el artículo 27.9 en relación con el artículo 32.2, letras a) y b), y 32.3, letras a) y b).
3. La evaluación de la conformidad se realizará conforme al artículo 32 del Reglamento de Ciberresiliencia, y la documentación técnica y la declaración UE de conformidad se regirán por los artículos 31 y 28, respectivamente.

Artículo 6. Autoridad notificante

1. El Centro Criptológico Nacional (en adelante, CCN), adscrito al Centro Nacional de Inteligencia del Ministerio de Defensa, es la autoridad notificante de España a efectos del Reglamento de Ciberresiliencia. Como tal, será responsable de establecer y aplicar los procedimientos para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como del seguimiento de los organismos notificados, incluida la supervisión de sus filiales y subcontratistas.
2. La autoridad notificante notificará a la Comisión Europea y a los demás Estados miembros los organismos autorizados para llevar a cabo las tareas de evaluación de la conformidad con arreglo al Reglamento de Ciberresiliencia, y comunicará sin demora cualquier modificación, restricción, suspensión o retirada de la notificación conforme al Derecho de la Unión.
3. La autoridad notificante actuará con independencia funcional y sin perjuicio de las competencias de la autoridad de vigilancia del mercado, pudiendo recabar la cooperación de otras autoridades u organismos públicos cuando sea necesario para el desempeño de sus funciones.
4. La autoridad notificante podrá basarse en certificados de acreditación emitidos por la Entidad Nacional de Acreditación (en adelante, ENAC), organismo nacional de acreditación designado por el Real Decreto 1715/2010, de 17 de diciembre, de conformidad con el Reglamento (CE) n.º 765/2008, como elemento de prueba del cumplimiento, por parte de un organismo de evaluación de la conformidad el sector público o del sector privado, de los requisitos aplicables. Asimismo, podrá encomendar a la ENAC tareas de apoyo técnico relacionadas con la evaluación de la competencia y el seguimiento de dichos organismos, sin perjuicio de que la autoridad notificante mantenga íntegramente la responsabilidad, el seguimiento continuado y la toma de decisiones sobre designación, notificación, restricción, suspensión o retirada de la notificación.
5. En ningún caso la acreditación o las tareas de apoyo mencionadas en el apartado anterior sustituirán las funciones propias de la autoridad notificante ni impedirán que ésta realice verificaciones adicionales, auditorías o requerimientos cuando lo considere necesario.
6. Cuando la autoridad notificante encomiende tareas de evaluación, notificación, supervisión o apoyo a una entidad distinta de un organismo público, dicha entidad deberá ser persona jurídica y cumplir los requisitos de independencia, imparcialidad y ausencia de conflictos de interés establecidos en el artículo 37 del Reglamento de Ciberresiliencia, así como adoptar las disposiciones pertinentes para asumir las responsabilidades derivadas de sus actividades. El instrumento jurídico habilitante preverá, en todo caso, obligaciones de confidencialidad y seguridad de la información, régimen de incompatibilidades y sujeción a las instrucciones de la autoridad notificante.
7. La autoridad notificante asumirá la plena responsabilidad de las tareas realizadas por las entidades de apoyo a que se refieren los apartados anteriores y de las decisiones que, en todo caso, le corresponden.
8. La autoridad notificante comunicará las notificaciones iniciales y sus modificaciones, restricciones, suspensiones o retirada de la notificación a

través del sistema de información "New Approach Notified and Designated Organisations (NANDO)" desarrollado y gestionado por la Comisión, conforme al artículo 43.2 del Reglamento de Ciberresiliencia, y mantendrá un registro nacional público de los organismos notificados, velando por su consistencia con la lista pública de la Comisión a que se refiere el artículo 44 del mismo Reglamento.

Artículo 7. Solicitud de notificación

1. Los organismos de evaluación de la conformidad, del sector público o del sector privado, establecidos en España que deseen ser notificados a efectos del Reglamento de Ciberresiliencia presentarán solicitud ante la autoridad notificante, de conformidad con su artículo 42. La solicitud podrá presentarse por los medios previstos en el artículo 16.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, Ley 39/2015) o a través de la sede electrónica u otros medios electrónicos que determine la autoridad notificante.
2. La solicitud incluirá una descripción de las actividades de evaluación de la conformidad, del o de los procedimientos aplicables y de los productos con elementos digitales para los que el organismo se declara competente, así como, cuando proceda, un certificado de acreditación expedido por ENAC, en su condición de organismo nacional de acreditación. A efectos de presunción de conformidad, la acreditación deberá haberse emitido con arreglo a las normas armonizadas pertinentes o a partes de las mismas, cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea, de acuerdo con el artículo R18 del anexo I de la Decisión n.º 768/2008/CE. Dicha acreditación conferirá presunción de conformidad con los requisitos del artículo 39 del Reglamento de Ciberresiliencia, en la medida en que dichas normas los cubran, conforme a su artículo 40.
3. Cuando no se aporte certificado de acreditación, el solicitante deberá motivar dicha circunstancia y acompañar su solicitud de toda la documentación necesaria para la verificación, reconocimiento y seguimiento periódico del cumplimiento de los requisitos del artículo 39 del Reglamento de Ciberresiliencia. La autoridad notificante podrá realizar las verificaciones adicionales que resulten precisas, incluidas evaluaciones in situ y auditorías documentales, cuando resulte necesario.
4. La autoridad notificante podrá requerir la subsanación o mejora de la solicitud de acuerdo con lo establecido en el artículo 68 de la Ley 39/2015.
5. El plazo máximo para resolver y notificar será de seis meses desde la presentación de la solicitud. Transcurrido dicho plazo sin resolución expresa, la solicitud podrá entenderse desestimada por silencio administrativo, de acuerdo con los artículos 21.2 y 24.2 de la Ley 39/2015, sin perjuicio de los plazos y actuaciones ulteriores previstos en el Reglamento de Ciberresiliencia para la oposición de la Comisión y de los Estados miembros en el procedimiento de notificación.
6. La descripción del alcance solicitado será coherente con los actos delegados que, en su caso, adopte la Comisión conforme al artículo 27.9 del Reglamento de Ciberresiliencia, sin incluir requisitos cuya evaluación por tercera parte haya

quedado eliminada por la expedición de un certificado europeo de ciberseguridad con nivel de garantía al menos “sustancial” en el marco de los esquemas europeos de certificación de la ciberseguridad.

Artículo 8. Recurso frente a las decisiones de los organismos notificados

1. Los organismos notificados deberán disponer de un procedimiento interno de apelación y gestión de reclamaciones, independiente e imparcial, frente a sus protocolos, actas, informes y decisiones de certificación, incluidas la denegación, restricción, suspensión o retirada de certificados. El procedimiento será accesible, fijará plazos razonables y concluirá mediante resolución motivada.
2. Sin perjuicio de lo anterior, los interesados podrán impugnar las decisiones de los organismos notificados ante la jurisdicción competente, garantizándose un procedimiento de recurso en los términos del artículo 48 del Reglamento de Ciberresiliencia.
3. Los interesados podrán asimismo presentar reclamación ante la autoridad notificante cuando consideren que el organismo notificado ha infringido sus obligaciones o procedimientos. La autoridad notificante podrá requerir información, exigir medidas correctoras y adoptar las medidas de supervisión que procedan, incluida la restricción, suspensión o retirada de la notificación, de conformidad con el Reglamento de Ciberresiliencia y la normativa nacional aplicable.
4. Contra las resoluciones que, en su caso, dicte la autoridad notificante en el ejercicio de sus potestades de supervisión, que ponen fin a la vía administrativa, podrá interponerse recurso potestativo de reposición en el plazo de un mes o recurso contencioso-administrativo en los términos de la Ley 29/1998, de 13 de julio.

Artículo 9. Vigilancia del mercado y control de productos con elementos digitales

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (en adelante, SETID), del Ministerio para la Transformación Digital y de la Función Pública, es la autoridad de vigilancia del mercado a efectos del Reglamento de Ciberresiliencia. La SETID actuará con independencia funcional y sin perjuicio de las competencias de otras autoridades.
2. La autoridad de vigilancia del mercado velará por que los productos con elementos digitales puestos a disposición en el mercado cumplan lo dispuesto en el Reglamento de Ciberresiliencia y en el Reglamento (UE) 2019/1020, adoptando las medidas necesarias para hacer cesar o remediar los incumplimientos, incluida la puesta en conformidad, retirada o recuperación y, en su caso, la prohibición o restricción de su comercialización.
3. En cumplimiento del artículo 52 del Reglamento de Ciberresiliencia, la autoridad de vigilancia del mercado, realizará, entre otras, las siguientes funciones:
    a) Informará a los consumidores de dónde notificar vulnerabilidades, incidentes y ciberamenazas y presentar reclamaciones que puedan indicar el incumplimiento del Reglamento de Ciberresiliencia y atenderá

las que reciba.

b) Publicará orientaciones y recomendaciones dirigidas a los operadores económicos.

c) Cooperará con otras autoridades competentes nacionales y de la Unión, con ENISA y con el CSIRT designado por España como coordinador en virtud del artículo 12, apartado 1, de la Directiva (UE) 2022/2555 (en adelante, CSIRT designado como coordinador).

d) Intercambiará información a través de los sistemas de la Unión aplicables, incluido ICSMS, y se coordinará con la oficina de enlace única prevista en el Reglamento (UE) 2019/1020.

e) Remitirá a la Comisión los informes y datos previstos sobre su actividad de vigilancia en el ámbito del Reglamento de Ciberresiliencia.

f) Participará en el ADCO específico del Reglamento de Ciberresiliencia, conforme al artículo 52.15 del mismo.

g) Supervisará, conforme al artículo 52.16 del Reglamento de Ciberresiliencia, cómo los fabricantes aplican los criterios del artículo 13.8 relativos al período de soporte, y colaborará en la publicación de estadísticas y orientaciones a que se refiere dicho precepto

4. En el ejercicio de las funciones que le atribuye el Reglamento sobre Ciberresiliencia, la autoridad de vigilancia del mercado contará con las facultades previstas en el artículo 14 del Reglamento (UE) 2019/1020, pudiendo, en particular:

    a) Solicitar muestras gratuitas para ensayo.

    b) Requerir documentación, especificaciones técnicas, datos e información, incluido el acceso al software incorporado en la medida imprescindible para evaluar la conformidad, y obtener copias de los soportes pertinentes.

    c) Requerir información sobre cadena de suministro, red de distribución, cantidades en el mercado y otros modelos con las mismas características técnicas, cuando sea pertinente.

    d) Determinar la titularidad de sitios web o interfaces en línea relacionados con el producto objeto de investigación y ordenar medidas sobre dichas interfaces, incluida la retirada o deshabilitación de contenidos relativos a ofertas no conformes, en los términos del Derecho de la Unión y nacional aplicable.

    e) Realizar actuaciones de comprobación y evaluaciones in situ conforme a la normativa nacional.

5. Cuando un producto que, aun cumpliendo el Reglamento de Ciberresiliencia, presente un riesgo para la salud o seguridad de las personas u otros intereses públicos protegidos, la autoridad de vigilancia del mercado exigirá al operador económico pertinente que elimine el riesgo o, en su caso, retire o recupere el producto en un plazo razonable y proporcional a la naturaleza del riesgo, de conformidad con los procedimientos de salvaguardia previstos en el Derecho de la Unión.
6. De conformidad con el artículo 15 del Reglamento (UE) 2019/1020, la autoridad de vigilancia del mercado podrá repercutir al operador económico pertinente la totalidad de los costes derivados de sus actuaciones en casos de

incumplimiento, incluidos, en su caso, los ensayos, almacenamiento y actuaciones relacionadas con productos declarados no conformes.

7. La autoridad de vigilancia del mercado cooperará con las autoridades aduaneras y con los servicios responsables de los controles en frontera exterior en los términos de los artículos 25 a 27 del Reglamento (UE) 2019/1020, y con la oficina de enlace única designada por España, a efectos de coordinación e intercambio de información.
8. El tratamiento de datos personales y la confidencialidad de la información obtenida en el ejercicio de estas funciones se ajustarán a la normativa de protección de datos y a las obligaciones de secreto aplicables. Las medidas que se adopten serán proporcionadas y motivadas.
9. Las medidas que se adopten lo serán sin perjuicio de las obligaciones de notificación previstas en los artículos 14 y 16 del Reglamento de Ciberresiliencia, así como de las que resulten de aplicación en materia de protección de datos personales.

Artículo 10. Coordinación en vulnerabilidades e incidentes

1. La autoridad de vigilancia del mercado y el CSIRT designado como coordinador colaborarán y, cuando proceda, actuarán conjuntamente en la divulgación coordinada de vulnerabilidades, así como en la recepción y tratamiento de las notificaciones de vulnerabilidades explotadas e incidentes graves relacionados con productos con elementos digitales, sin perjuicio de las obligaciones que correspondan a los operadores económicos conforme al Derecho de la Unión. A la vista de dicha información, el CSIRT designado como coordinador podrá determinar, en coordinación con la autoridad de vigilancia del mercado y dentro de su ámbito competencial, las medidas adecuadas para atenuar los riesgos derivados de tales vulnerabilidades e incidentes, sin perjuicio de las competencias de otros CSIRT u otras autoridades competentes.
2. Cuando las actuaciones anteriores impliquen datos personales, la autoridad de vigilancia del mercado cooperará con la Agencia Española de Protección de Datos, sin perjuicio de las obligaciones de notificación que correspondan a los responsables del tratamiento conforme a la normativa de protección de datos.
3. La información se intercambiará con respeto a la confidencialidad, a la normativa de protección de datos y, en su caso, al régimen de información clasificada, procurando una comunicación pública coherente y proporcional al riesgo.

Artículo 11. Oficina de enlace única

1. La Dirección General de Consumo, del Ministerio de Derechos Sociales, Consumo y Agenda 2030, es la oficina de enlace única a efectos del Reglamento (UE) 2019/1020, que ejercerá a través de la Subdirección General de Coordinación, Calidad y Cooperación en Consumo, conforme a lo previsto en el artículo 7.2, letra ñ) del Real Decreto 209/2024, de 27 de febrero.

2. La oficina de enlace única ejercerá las funciones de representación y asistencia que le atribuye el artículo 10.4 del Reglamento (UE) 2019/1020.

3. La oficina de enlace única introducirá y mantendrá la información que le corresponda en el sistema de información y comunicación a que se refiere el artículo 34 del Reglamento (UE) 2019/1020 (ICSMS).

4. La oficina de enlace única participará en la Red de la Unión sobre Conformidad de los Productos, de acuerdo con los artículos 29 y 30 del Reglamento (UE) 2019/1020.

Artículo 12. Principios generales y reglas del marcado CE

1. El marcado CE se regirá por los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

2. En lo específico del Reglamento de Ciberresiliencia, el marcado CE se ajustará a lo dispuesto en sus artículos 29 y 30, sin perjuicio de los actos delegados o de ejecución que, en su caso, se adopten.

3. La autoridad de vigilancia del mercado adoptará las medidas que procedan en caso de uso indebido del marcado CE o de marcados, signos o inscripciones que puedan inducir a error respecto al significado o la forma del marcado CE, de conformidad con el Reglamento de Ciberresiliencia, el Reglamento (UE) 2019/1020, el Reglamento (CE) n.º 765/2008 y la normativa nacional aplicable.

Artículo 13. Comisión de coordinación del Reglamento de Ciberresiliencia

1. Se crea la Comisión de coordinación del Reglamento de Ciberresiliencia como órgano colegiado interministerial de cooperación entre la autoridad de vigilancia del mercado y la autoridad notificante.

2. La adscripción administrativa, composición y régimen de funcionamiento de la Comisión de coordinación del Reglamento de Ciberresiliencia se establecerán mediante orden conjunta de las personas titulares del Ministerio para la Transformación Digital y de la Función Pública y del Ministerio de Defensa, sin incremento de gasto público.

Artículo 14. Cooperación entre la autoridad de vigilancia del mercado y la autoridad notificante

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y el Centro Criptológico Nacional cooperarán de forma estable para asegurar una aplicación coherente del Reglamento de Ciberresiliencia, evitando solapamientos y duplicidades.

2. En el plazo máximo de seis meses desde la entrada en vigor del presente real decreto, ambas autoridades aprobarán conjuntamente un protocolo operativo de cooperación que fijará canales de comunicación, puntos de contacto, criterios básicos de intercambio de información y mecanismos de resolución de discrepancias.

3. La cooperación se realizará con respeto a la confidencialidad, a la normativa de protección de datos y, cuando proceda, al régimen de información clasificada, sin perjuicio del ejercicio de las competencias propias de cada autoridad.

Artículo 15. Medidas de apoyo a las empresas

1. De conformidad con el artículo 33 del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia), la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en colaboración y coordinación con la S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), podrá emprender, cuando proceda, acciones dirigidas a las microempresas y las pequeñas y medianas empresas, incluidas las empresas emergentes, que podrán comprender, entre otras:

a) Organizar actividades específicas de sensibilización y formación sobre la aplicación del Reglamento de Ciberresiliencia;

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 preguntas sobre su aplicación;

c) Apoyar actividades de prueba y evaluación de la conformidad, también, cuando proceda, con el apoyo del Centro Europeo de Competencia en Ciberseguridad y la Red de Centros Nacionales de Coordinación, creados por el Reglamento (UE) 2021/887.

2. Estas actuaciones se articularán preferentemente a través de herramientas y recursos existentes, tales como guías, plantillas, formación en línea y canales de consulta, y no generarán derechos subjetivos para los operadores económicos.

3. Las actuaciones previstas en este artículo se realizarán con cargo a los medios personales y materiales disponibles y, en su caso, con fondos europeos o instrumentos ya existentes, sin que el presente real decreto suponga compromiso de gasto ni la creación de nuevas líneas de subvenciones.

Disposición derogatoria única. Derogación normativa.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en este real decreto.

Disposición transitoria única. Actuaciones preparatorias

Hasta las fechas de aplicación previstas en el Reglamento de Ciberresiliencia, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, como autoridad de vigilancia del mercado, y el Centro Criptológico Nacional, como autoridad notificante, podrán realizar las actuaciones preparatorias necesarias para la puesta en marcha de los procedimientos y mecanismos de cooperación previstos en dicho Reglamento y en este real decreto.

Disposición adicional primera. Información a efectos de vigilancia del mercado

Mediante orden de la persona titular del Ministerio para la Transformación Digital y de la Función Pública podrá establecerse la comunicación previa o periódica de datos identificativos del operador económico responsable exclusivamente para fines de vigilancia del mercado, respecto de categorías de productos o supuestos que se determinen, garantizando el principio de proporcionalidad y la consistencia con el Reglamento (UE) 2019/1020. La comunicación no constituirá requisito para la comercialización de los productos.

Disposición adicional segunda. Laboratorio técnico de apoyo preferente

1. Se designa a la S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE) como laboratorio técnico de apoyo preferente de la autoridad de vigilancia del mercado en materia de productos con elementos digitales.

2. La colaboración de INCIBE con la autoridad de vigilancia del mercado incluirá, al menos:

    a) La realización de ensayos y análisis técnicos sobre productos con elementos digitales obtenidos en actuaciones de vigilancia del mercado (incluidas las acciones de control simultáneas coordinadas —«barridos»— a que se refiere el artículo 60 del Reglamento de Ciberresiliencia, muestras, adquisiciones —incluidas, cuando proceda, bajo identidad encubierta, conforme al mismo precepto—, retiradas o recuperaciones).
    b) La evaluación técnica de vulnerabilidades y, en su caso, de los aspectos técnicos de la conformidad o no conformidad con los requisitos aplicables, así como de las medidas de corrección adoptadas por los operadores económicos.
    c) La emisión de informes técnicos no vinculantes sobre la documentación técnica y las certificaciones aportadas por los operadores económicos, sin perjuicio de las competencias de la autoridad notificante en la supervisión de organismos notificados.
    d) Actuaciones de apoyo técnico, información y sensibilización, así como la recepción y canalización de avisos y quejas relacionadas con

productos con elementos digitales.

e) Las demás tareas instrumentales de carácter técnico que resulten necesarias para el ejercicio de las funciones de vigilancia del mercado previstas en el Reglamento (UE) 2019/1020 y en el Reglamento de Ciberresiliencia.

3. Los ensayos y análisis técnicos necesarios se realizarán preferentemente en el laboratorio de INCIBE. Cuando resulte necesario por razones de capacidad, especialidad, independencia o urgencia, INCIBE podrá subcontratar la ejecución de dichos ensayos y análisis a laboratorios especializados que reúnan las condiciones técnicas adecuadas. Asimismo, la autoridad de vigilancia del mercado podrá, cuando lo considere más adecuado para el eficaz y eficiente ejercicio de sus funciones, contratar directamente otros laboratorios que cumplan esas mismas condiciones. Los informes tendrán carácter técnico y no vinculante.

4. Esta designación no atribuye potestades públicas ni facultades decisorias a INCIBE ni limita la facultad de la autoridad para utilizar otros laboratorios cuando se justifique. Los costes de actuaciones relativas a productos no conformes podrán repercutirse a los operadores responsables, conforme al artículo 15 del Reglamento (UE) 2019/1020.

5. En el funcionamiento del laboratorio de INCIBE, de los laboratorios que este subcontrate y de los que contrate directamente la autoridad de vigilancia del mercado, se garantizarán la confidencialidad, la protección de datos y, cuando proceda, el régimen de información clasificada, así como la trazabilidad y cadena de custodia de las muestras, la integridad y seguridad de la información y de los soportes (con controles de acceso y registro de operaciones), la conservación de registros y la reproducibilidad de resultados, y la gestión de conflictos de interés e independencia técnica. Las muestras se devolverán o destruirán según proceda, dejando constancia. Estas garantías se articularán a través del sistema de gestión de la calidad del laboratorio

Disposición final primera. Título competencial.

Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.10.ª, 13.ª, 21.ª y 29.ª de la Constitución, que atribuye al Estado la competencia exclusiva sobre el comercio exterior, las bases y coordinación de la planificación general de la actividad económica, las telecomunicaciones, y la seguridad pública.

Disposición final segunda. Desarrollo y aplicación de este real decreto.

Se habilita a la persona titular del Ministerio para la Transformación Digital y de la Función Pública y, en su ámbito competencial, a la persona titular del Ministerio de Defensa, para dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de este real decreto.

Disposición final tercera. Entrada en vigor.

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado»