MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL PROYECTO DE REAL DECRETO POR EL QUE SE DESIGNA 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) Nº 168/2013 Y EL REGLAMENTO (UE) 2019/1020 Y LA DIRECTIVA (UE) 2020/1828 (REGLAMENTO DE CIBERRESILIENCIA)

Madrid, 22 de noviembre de 2025

Contenido

MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL PROYECTO DE REAL DECRETO POR EL QUE SE DESIGNA 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) Nº 168/2013 Y EL REGLAMENTO (UE) 2019/1020 Y LA DIRECTIVA (UE) 2020/1828 (REGLAMENTO DE CIBERRESILIENCIA)

1. RESUMEN EJECUTIVO

Ministerios / Órganos proponentes	Ministerio para la Transformación Digital y de la Función Pública.	**Fecha**	Diciembre 2025
Título de la norma	Real Decreto por el que se designa 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) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) .		
Tipo de memoria	☑ **Normal** ☐ **Abreviada**		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	Las obligaciones impuestas a España como Estado miembro por 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 (Reglamento de Ciberresiliencia).		

Objetivos que se persiguen	- Designar la autoridad de vigilancia del mercado responsable de supervisar el cumplimiento del Reglamento de Ciberresiliencia en España. - Designar la autoridad notificante y establecer los procedimientos de evaluación, designación, notificación y supervisión de los organismos de evaluación de la conformidad previstos en el Reglamento de Ciberresiliencia. - Integrar el despliegue del Reglamento de Ciberresiliencia en el marco general de vigilancia de mercado del Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.° 765/2008 y (UE) n.° 305/2011, así como en la arquitectura institucional española de ciberseguridad. - Definir el papel de ENAC como organismo nacional de acreditación y el de INCIBE como laboratorio de apoyo preferente en materia de ensayos y análisis técnicos, sin atribución de potestades públicas. - Establecer canales de coordinación e intercambio de información entre la autoridad de vigilancia del mercado, la autoridad notificante, el CSIRT coordinador de vulnerabilidades y el resto de autoridades nacionales, incluyendo el uso de las plataformas europeas de información. - Asegurar que España cumple en plazo las obligaciones organizativas y de coordinación impuestas por el Reglamento de Ciberresiliencia, evitando la creación de nuevas cargas administrativas o requisitos nacionales adicionales para los operadores económicos.
Principales alternativas consideradas	El Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia) es directamente aplicable y obliga a los Estados miembros a designar autoridades de vigilancia de mercado y notificante, y a organizar determinados mecanismos de coordinación y vigilancia de mercado. Por ello, no existe alternativa a la adopción de una norma de derecho interno para el cumplimiento de estas obligaciones. . Se han valorado distintas opciones en cuanto al instrumento normativo a adoptar y al modelo de gobernanza. Se ha optado por un real decreto específico que concentre la designación de la autoridad de vigilancia del mercado y de la autoridad notificante, la articulación del papel de ENAC e INCIBE y los mecanismos de coordinación, por ser la opción más coherente con el Reglamento (UE) 2019/1020 y ofrecer mayor seguridad jurídica a operadores y autoridades..

CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Real Decreto
Estructura de la norma	El proyecto se estructura en una exposición de motivos, quince artículos, dos disposiciones adicionales, una disposición transitoria única, una disposición derogatoria única y tres disposiciones finales.
Informes	De acuerdo con la Ley 50/1997, de 27 de noviembre, del Gobierno, y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se prevé recabar informes de: • Ministerio de Defensa (artículo 26.5.1ª de la Ley 50/1997). • Ministerio de Economía, Comercio y Empresa (artículo 26.5.1ª de la Ley 50/1997). . • Ministerio de Industria y Turismo (artículo 26.5.1ª de la Ley 50/1997).. • Agencia Española de Protección de Datos (artículo 26.5.1ª de la Ley 50/1997).. • Oficina de Coordinación y Calidad Normativa (artículo 26.9 de la Ley 50/1997). • Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública (artículo 26.5.4ª de la Ley 50/1997). También debe recabarse la aprobación previa del Ministerio de Hacienda (art. 26.5. de la Ley 50/1997). Por último, debe recabarse el dictamen del Consejo de Estado, en los términos previstos en su Ley Orgánica.
Participación pública	. El proyecto ha sido sometido a un trámite de consulta pública realizado en la sede electrónica del MTDFP desde el día 1 de diciembre de 2025 hasta el día 17 de diciembre de 2025. El proyecto debe someterse al trámite de audiencia pública e información pública

<table>
<tr><th colspan="3">ANÁLISIS DE IMPACTOS</th></tr>
<tr><td>ADECUACIÓN AL ORDEN DE COMPETENCIAS</td><td colspan="2">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 Española, 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.

La norma se limita a designar las autoridades estatales de vigilancia del mercado y notificante a efectos del Reglamento de Ciberresiliencia , a articular su participación en los mecanismos europeos de vigilancia del mercado y a establecer los canales de coordinación interna necesarios para la aplicación del citado Reglamento, sin regular aspectos propios de la organización o la prestación de servicios por parte de las comunidades autónomas o las entidades locales.</td></tr>
<tr><td>IMPACTO ECONÓMICO Y PRESUPUESTARIO</td><td>Efectos sobre la economía en general.</td><td>El real decreto tiene un impacto económico muy limitado, ya que no introduce requisitos técnicos adicionales ni nuevas obligaciones materiales para los operadores económicos más allá de las que impone directamente el Reglamento de Ciberresiliencia. Su efecto principal es organizar, en el ámbito interno, la designación de autoridades y los mecanismos de coordinación, lo que aporta seguridad jurídica y previsibilidad a los fabricantes, importadores y distribuidores de productos con elementos digitales..</td></tr>
</table>

	En relación con la competencia	☒ La norma no tiene efectos significativos sobre la competencia. ☐ La norma tiene efectos positivos sobre la competencia. ☐ La norma tiene efectos negativos sobre la competencia.
	Desde el punto de vista de las cargas administrativas	☐ Supone una reducción de cargas administrativas. ☐ Incorpora nuevas cargas administrativas. ☒ No afecta a las cargas administrativas.
	Desde el punto de vista de los presupuestos, la norma ☐ Afecta a los presupuestos de la Administración del Estado. ☐ Afecta a los presupuestos de otras Administraciones Territoriales.	☐ Implica un gasto. *(en el sistema de vigilancia ya existente)* ☐ Implica un ingreso.
IMPACTO DE GÉNERO	La norma tiene un impacto de género	☐ Negativo ☒ Nulo ☐ Positivo

IMPACTO EN MATERIA DE INFANCIA, ADOLESCENCIA Y FAMILIA	La norma tiene un impacto en la infancia, adolescencia y familia:	☐ Negativo ☒ Nulo ☐ Positivo
IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES	La norma tiene un impacto en la protección de datos personales:	☐ Negativo ☐ Nulo ☒ Positivo
OTROS IMPACTOS CONSIDERADOS	No existen otros impactos significativos de carácter ambiental. En materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, el impacto es nulo.	
EVALUACIÓN "EX POST"	Sí procede. Se prevé una evaluación ex post a los tres años desde la entrada en vigor del real decreto, coordinada por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, para analizar el grado de cumplimiento de los objetivos del Reglamento de Ciberresiliencia, la adecuación de la organización institucional (AVM, autoridad notificante y laboratorio de apoyo) y la eficiencia en el uso de los recursos asignados.	

2. OPORTUNIDAD DE LA PROPUESTA

2.1. Motivación / situación que se regula

2.1.1. Causas de la propuesta (mandato UE / necesidad interna)

- 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 modifican el Reglamento (UE) nº 168/2013, el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (en adelante, Reglamento de Ciberresiliencia o CRA), establece un marco directamente aplicable en todos los Estados miembros. Este Reglamento impone a los Estados miembros, entre otras obligaciones: Designar una autoridad de vigilancia del mercado a efectos del CRA, en el marco del Reglamento (UE) 2019/1020, responsable de supervisar el cumplimiento de los requisitos esenciales de ciberseguridad por parte de los operadores económicos.
- Designar una autoridad notificante, encargada de establecer y aplicar los procedimientos de evaluación, designación, notificación y supervisión de los organismos de evaluación de la conformidad.
- Asegurar que existen capacidades técnicas suficientes, incluidos laboratorios y sistemas de información, para realizar ensayos, análisis y actuaciones de vigilancia del mercado, así como para intercambiar información con la Comisión y el resto de Estados miembros.

Actualmente, conforme al ordenamiento jurídico español:

- La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID) ejerce funciones de autoridad de vigilancia del mercado en ámbitos afines; por ejemplo, en la aplicación del Reglamento Delegado (UE) 2022/30 de la Comisión de 29 de octubre de 2021 que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, apartado 3, letras d), e) y f), de dicha Directiva (Reglamento Delegado (UE) 2022/30), que introduce requisitos de ciberseguridad en determinados equipos radioeléctricos.
- El Centro Criptológico Nacional (CCN) ostenta la condición de Autoridad Nacional de Certificación de la Ciberseguridad al amparo del 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) nº 526/2013 («Reglamento sobre la Ciberseguridad»), acumulando experiencia en evaluación de productos TIC.

- El Instituto Nacional de Ciberseguridad de España, M.P. (INCIBE) dispone de capacidades técnicas y de laboratorio y ya actúa como Centro de Coordinación Nacional (NCC-ES) del Centro Europeo de Competencia en Ciberseguridad.

Por tanto, la propuesta de real decreto responde a la necesidad de ordenar y formalizar este modelo de gobernanza a la luz del CRA, integrándolo al mismo tiempo en el régimen general de vigilancia del mercado del Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.° 765/2008 y (UE) n.° 305/2011 (Reglamento (UE) 2019/1020)..

2.1.2. Colectivos afectados

Los colectivos afectados por la norma son:

- Operadores económicos que comercializan en el mercado español productos con elementos digitales incluidos en el ámbito de aplicación del CRA (fabricantes, importadores, distribuidores y representantes autorizados), toda vez que el proyecto normativo designa a las autoridades españolas que ejercerán la vigilancia del mercado y la notificación de organismos de evaluación de la conformidad.
- Organismos de evaluación de la conformidad y laboratorios que aspiren a intervenir en la evaluación de productos CRA, incluidos organismos públicos y privados:

De forma indirecta, se ven también afectados:

- Los usuarios finales y consumidores, que resultan beneficiados por una mayor seguridad de los productos con elementos digitales.
- El conjunto del tejido empresarial que depende de estos productos para la prestación de servicios, al disminuir la probabilidad e impacto de incidentes de ciberseguridad.

Por su parte, las administraciones públicas y los organismos públicos implicados en la aplicación del CRA son:

  - La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID), como autoridad de vigilancia del mercado.
  - El Centro Criptológico Nacional (CCN), como autoridad notificante.
  - INCIBE, como laboratorio de apoyo preferente.
  - ENAC, como organismo nacional de acreditación.

2.1.3. Interés público implicado

La norma proyectada incide en varios intereses públicos de primer nivel:

- La ciberseguridad y la resiliencia digital, al contribuir a que los productos con elementos digitales comercializados en España cumplan los requisitos de seguridad por diseño y por defecto establecidos en el CRA, reduciendo vulnerabilidades y facilitando la gestión de incidentes.
- El correcto funcionamiento del mercado interior y la competitividad de la economía, al proporcionar un marco claro y previsible a fabricantes y otros operadores económicos, alineado con las reglas comunes de la Unión Europea.
- La seguridad pública y la protección de infraestructuras críticas y servicios esenciales, en la medida en que muchos de estos servicios dependen de productos con elementos digitales que deben ser robustos frente a ciberataques.
- La protección de los datos personales y otros activos intangibles, dado que el CRA incluye requisitos destinados a que los productos solo procesen los datos necesarios para sus funciones previstas y que lo hagan de forma segura.
- El cumplimiento por España de sus obligaciones derivadas del Derecho de la Unión Europea, evitando procedimientos de infracción y garantizando una aplicación uniforme y coordinada del CRA.

2.2. Objetivos

2.2.1. Objetivo general

El objetivo general del proyecto de real decreto es garantizar la aplicación eficaz, coherente y eficiente en España del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia) en los aspectos que requieren una decisión de organización interna por parte de los Estados miembros, sin introducir requisitos técnicos adicionales ni nuevas obligaciones materiales para los operadores económicos más allá de las previstas en dicho Reglamento.

2.2.2. Objetivos específicos

En desarrollo de este objetivo general, la norma persigue, en particular:

- Designar la autoridad de vigilancia del mercado en el ámbito del CRA, integrando sus funciones en el régimen de vigilancia del mercado del Reglamento (UE) 2019/1020 y en la estructura institucional existente en materia de telecomunicaciones y servicios digitales.

- Designar la autoridad notificante a efectos del CRA, precisando sus funciones en materia de evaluación, designación, notificación y supervisión de los organismos de evaluación de la conformidad, de acuerdo con los artículos 36 a 41 del Reglamento.
- Articular el papel del organismo nacional de acreditación (ENAC) como instrumento técnico de apoyo para verificar el cumplimiento de los requisitos exigidos a los organismos de evaluación de la conformidad, en los términos previstos por el CRA y el Reglamento (CE) nº 765/2008.
- Designar a INCIBE como laboratorio de apoyo preferente de la autoridad de vigilancia del mercado, reconociendo sus capacidades técnicas en materia de ciberseguridad y ensayos sobre productos con elementos digitales, sin atribuirle potestades públicas ni facultades decisorias.
- Establecer mecanismos de coordinación e intercambio de información entre la autoridad de vigilancia del mercado, la autoridad notificante, los CSIRTs competentes, la Agencia Española de Protección de Datos y otras autoridades nacionales implicadas, así como con la Comisión Europea y las autoridades de otros Estados miembros, incluyendo el uso de los sistemas de información europeos (ICSMS, NANDO, sistemas de notificación de incidentes, etc.).
- Evitar solapamientos y lagunas competenciales entre las diferentes autoridades nacionales, asegurando una aplicación coherente del CRA y un punto de contacto claro para los operadores económicos.
- Minimizar los costes administrativos y organizativos adicionales, aprovechando las capacidades ya existentes en la Administración General del Estado y sus organismos públicos, de forma que los costes derivados del CRA se gestionen de la manera más eficiente posible.

2.3. Análisis de alternativas

2.3.1. Alternativa cero (no intervención)

La alternativa de no intervención normativa resulta descartable al tratarse de una propuesta normativa necesaria para la aplicación en España del Reglamento de Ciberresiliencia.

2.3.2. Alternativas normativas

Se valoraron distintas opciones en cuanto al instrumento normativo a adoptar; en particular, una norma con rango de ley, diversas órdenes ministeriales de ámbito sectorial, la modificación de normas sectoriales ya existentes o aprobar un único real decreto.

Esta última alternativa se considera el instrumento jurídico más idóneo al ofrecer un marco único y coherente con el Reglamento (UE) 2019/1020 para las designaciones de autoridades y mecanismos de coordinación exigidos por el Reglamento de Ciberresiliencia.

2.4. Adecuación a los principios de buena regulación

El proyecto normativo 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 la norma permite dar cumplimiento a las obligaciones impuestas a los Estados miembros por el Reglamento de Ciberresiliencia, que impone designar autoridades competentes y organizar la vigilancia del mercado.

En cuanto al cumplimiento del principio de proporcionalidad, la 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.

2.5. Plan Anual Normativo

2.5.1. Inclusión en el Plan Anual Normativo

La iniciativa figura en el Plan Anual Normativo de la Administración General del Estado para 2025, dentro del apartado correspondiente al Ministerio para la Transformación Digital y de la Función Pública, como real decreto de desarrollo del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia), con previsión de elevación al Consejo de Ministros en el último trimestre de 2025.

3. CONTENIDO Y ANÁLISIS JURÍDICO

3.1. Contenido

3.1.1. Tipo de norma

Se trata de un real decreto que:

- aplica determinados aspectos organizativos del Reglamento de Ciberresiliencia, designando autoridades competentes, articulando su cooperación y concretando el uso de sistemas de información y capacidades técnicas,

- no introduce requisitos técnicos adicionales para los productos con elementos digitales, ni crea nuevas obligaciones materiales para los operadores económicos más allá de las previstas directamente en el CRA.

Su contenido es, por tanto, principalmente de organización administrativa y coordinación interna, en el marco de las competencias exclusivas del Estado en materia de comercio exterior, bases y coordinación de la planificación general de la actividad económica, telecomunicaciones y seguridad pública.

3.1.2. Estructura de la norma

El proyecto se estructura en un preámbulo, quince artículos y: dos disposiciones adicionales, una disposición transitoria única, una disposición derogatoria única y tres disposiciones finales.

- Artículos 1 a 3: objeto, definiciones y ámbito de aplicación.
    - El artículo 1 define el objeto: designar la Autoridad de Vigilancia del Mercado y la Autoridad Notificante a efectos del CRA y articular su marco básico de cooperación y coordinación, en coherencia con el Reglamento (UE) 2019/1020.
    - El artículo 2 remite, para las definiciones, al artículo 3 del CRA y, supletoriamente, al Reglamento (UE) 2019/1020 y a los actos delegados y de ejecución del CRA.
    - El artículo 3 delimita el ámbito de aplicación del real decreto a los productos con elementos digitales incluidos en el ámbito del CRA introducidos o puestos a disposición en el mercado español, excluyendo los productos excluidos por el artículo 2 del CRA y aquellos sometidos a regímenes de aplicación preferente en otros actos de la Unión.
- Artículos 4 y 5: obligaciones de operadores económicos y presunción de conformidad.
    - El artículo 4 se limita a remitir a las obligaciones del capítulo II del CRA (incluida la gestión de vulnerabilidades y obligaciones de información), aclarando que se aplican

sin perjuicio del Derecho de la Unión y nacional adicionales (por ejemplo, el Reglamento de maquinaria).

- El artículo 5 desarrolla la presunción y evaluación de la conformidad:
  - remisión a normas armonizadas y especificaciones comunes,
  - reconocimiento del papel de los esquemas europeos de certificación de ciberseguridad conforme al Reglamento (UE) 2019/881,
  - remisión expresa a los artículos 27, 28, 31 y 32 del CRA sobre documentación técnica, declaración UE de conformidad y módulos de evaluación.

- Artículos 6 a 8: autoridad notificante y régimen de organismos notificados.
  - El artículo 6 designa al Centro Criptológico Nacional (CCN) como autoridad notificante a efectos del CRA, detalla sus funciones (evaluación, designación, notificación y seguimiento de organismos notificados) y regula:
    - el uso de certificados de acreditación de ENAC como prueba de cumplimiento de requisitos,
    - la posibilidad de encomendar a ENAC tareas de apoyo técnico,
    - las condiciones para encomendar tareas a otras entidades (independencia, imparcialidad, ausencia de conflictos, responsabilidad, etc.),
    - la plena responsabilidad de la autoridad notificante sobre las tareas encomendadas y sus decisiones, y
    - el uso del sistema NANDO y el mantenimiento de un registro nacional de organismos notificados.
  - El artículo 7 regula la solicitud de notificación por parte de organismos de evaluación de la conformidad del sector público o privado establecidos en España: contenido mínimo, aportación de acreditación de ENAC o documentación equivalente, verificaciones adicionales y plazo para resolver, con remisión al silencio desestimatorio y coherencia con los actos delegados del CRA.
  - El artículo 8 establece el régimen de recurso frente a las decisiones de los organismos notificados: obligación de disponer de procedimientos internos de apelación, posibilidad de impugnar ante la jurisdicción competente y reclamación ante la autoridad notificante, que podrá adoptar medidas de supervisión, incluida la restricción, suspensión o retirada de la notificación.

- Artículos 9 y 10: autoridad de vigilancia del mercado y coordinación en vulnerabilidades e incidentes.
  - El artículo 9 designa a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID) como autoridad de vigilancia del mercado a efectos del CRA, define sus funciones en aplicación del artículo 52 del CRA y del Reglamento (UE) 2019/1020 (información a consumidores, publicación de orientaciones, cooperación con otras autoridades y ENISA, intercambio de información vía ICSMS, participación en el ADCO del CRA, supervisión de períodos de soporte, etc.) y detalla sus facultades de inspección y reacción (muestreo, requerimientos de información,

actuaciones in situ, medidas frente a riesgos y repercusión de costes en caso de incumplimiento).

- El artículo 10 regula la coordinación en vulnerabilidades e incidentes:
  - colaboración entre la autoridad de vigilancia del mercado y el CSIRT designado como coordinador conforme a NIS2 en la divulgación coordinada de vulnerabilidades y en la gestión/notificación de incidentes graves,
  - cooperación con la Agencia Española de Protección de Datos cuando intervengan datos personales,
  - garantías de confidencialidad, protección de datos e información clasificada.

- Artículo 11: oficina de enlace única. El artículo 11 identifica a la Dirección General de Consumo como oficina de enlace única a efectos del Reglamento (UE) 2019/1020 (ya designada por el RD 209/2024) y precisa sus funciones: representación y asistencia, carga de información en ICSMS y participación en la Red de la Unión sobre Conformidad de los Productos.
- Artículo 12: principios generales y reglas del marcado CE. El artículo 12 recuerda que el marcado CE se rige por el Reglamento (CE) nº 765/2008 y detalla que, en lo específico del CRA, se aplican sus artículos 29 y 30, facultando a la autoridad de vigilancia del mercado para actuar frente a usos indebidos o confusos de marcados y signos.
- Artículo 13: Comisión de coordinación del Reglamento de Ciberresiliencia. El artículo 13 crea una Comisión de coordinación del Reglamento de Ciberresiliencia como órgano colegiado interministerial de cooperación entre la autoridad de vigilancia del mercado y la autoridad notificante, cuya composición y funcionamiento se determinarán mediante orden conjunta de los Ministerios para la Transformación Digital y de la Función Pública y de Defensa, sin incremento de gasto público.
- Artículo 14: cooperación entre la autoridad de vigilancia del mercado y la autoridad notificante. El artículo 14 impone un deber de cooperación estable entre SETID y CCN para aplicar el CRA de manera coherente, evitando solapamientos, y prevé la aprobación conjunta, en seis meses, de un protocolo operativo de cooperación (canales, puntos de contacto, intercambio de información y resolución de discrepancias).
- Artículo 15: medidas de apoyo a las empresas. El artículo 15 desarrolla el artículo 33 del CRA sobre apoyo a microempresas y pequeñas empresas, facultando a la SETID, en coordinación con INCIBE, para emprender acciones de sensibilización, formación, acompañamiento y apoyo a actividades de prueba y evaluación, sin generar derechos subjetivos ni nuevas líneas de subvención y utilizando preferentemente herramientas y recursos existentes.

- Disposición derogatoria única. Deroga las disposiciones de igual o inferior rango que se opongan a lo establecido en el real decreto.
- Disposición transitoria única (Actuaciones preparatorias). Permite que la autoridad de vigilancia del mercado (SETID) y la autoridad notificante (CCN) realicen actuaciones

preparatorias antes de las fechas de aplicación del CRA, para poner en marcha procedimientos y mecanismos de cooperación, garantizando así una transición ordenada.

- Disposición adicional primera (Información a efectos de vigilancia del mercado). Habilita a la persona titular del Ministerio para la Transformación Digital y de la Función Pública para establecer, mediante orden ministerial, la comunicación previa o periódica de datos identificativos del operador económico exclusivamente para fines de vigilancia del mercado, respecto de determinadas categorías de productos o supuestos, garantizando proporcionalidad y consistencia con el Reglamento (UE) 2019/1020 y dejando claro que dicha comunicación no es requisito para la comercialización de los productos.
  Disposición adicional segunda (Laboratorio técnico de apoyo preferente). Designa a INCIBE como laboratorio técnico de apoyo preferente de la autoridad de vigilancia del mercado en materia de productos con elementos digitales.
- Disposición final primera (Título competencial). Precisa que el real decreto se dicta al amparo de los artículos 149.1.10.ª, 13.ª, 21.ª y 29.ª de la Constitución (comercio exterior, bases y coordinación de la planificación general de la actividad económica, telecomunicaciones y seguridad pública).
- Disposición final segunda (Desarrollo y aplicación). Habilita a las personas titulares del Ministerio para la Transformación Digital y de la Función Pública y del Ministerio de Defensa para dictar las disposiciones necesarias para el desarrollo y ejecución del real decreto en su respectivo ámbito competencial.
- Disposición final tercera (Entrada en vigor). Establece la entrada en vigor del real decreto el día siguiente al de su publicación en el «Boletín Oficial del Estado».

3.2. Análisis jurídico

3.2.1. Fundamento jurídico. Congruencia con el ordenamiento de la Unión Europea y con el ordenamiento jurídico español

El fundamento jurídico inmediato del proyecto de real decreto se encuentra en 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 (Reglamento de Ciberresiliencia o CRA), que fija:

- obligaciones técnicas y de gestión de riesgos para fabricantes y demás operadores económicos;

- requisitos esenciales de ciberseguridad, documentación técnica, marcado CE y evaluación de la conformidad;
- obligaciones de notificación de vulnerabilidades e incidentes.

De conformidad con el citado Reglamento corresponde a los Estados miembros:

- designación de autoridades competentes (vigilancia del mercado y notificación);
- organización de la cooperación interna entre autoridades;
- elección de laboratorios y organismos de evaluación de la conformidad, dentro del marco de los artículos 36 a 41 del CRA y el Reglamento 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;
- medidas de apoyo a microempresas y pequeñas empresas (artículo 33 CRA).

Asimismo, el proyecto de real decreto se apoya en el Reglamento (UE) 2019/1020 (relativo a la vigilancia del mercado y a la conformidad de los productos), en el Reglamento (CE) nº 765/2008 (sobre acreditación y vigilancia del mercado) y, en lo que respecta al papel del CCN e INCIBE, en el Reglamento (UE) 2019/881 (Cybersecurity Act) y el Reglamento (UE) 2021/887 (Centro Europeo de Competencia en Ciberseguridad y Red de NCC), que reconocen a estos organismos funciones específicas en materia de ciberseguridad.

Además, el proyecto de real decreto tiene en cuenta normas estatales ya vigentes que atribuyen funciones a los órganos designados:

- el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, que le asigna funciones como autoridad nacional de certificación de la seguridad de las TIC;
- el Real Decreto 1715/2010, de 17 de diciembre, que designa a ENAC como organismo nacional de acreditación;
- el Real Decreto 209/2024, de 27 de febrero, que designa a la Dirección General de Consumo como oficina de enlace única a efectos del Reglamento (UE) 2019/1020;
- y la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que configura las competencias de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, incluyendo funciones en materia de redes, servicios digitales y ciberseguridad del entorno privado.

3.2.2. Entrada en vigor

De conformidad con la disposición final tercera, el real decreto entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

Esta regla es congruente con el artículo 23 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y se considera adecuada para:

- asegurar la disponibilidad inmediata de las designaciones de autoridades y mecanismos de coordinación,
- permitir que estas autoridades puedan acometer las actuaciones preparatorias previstas en la disposición transitoria única antes de las fechas de aplicación del CRA, reduciendo el riesgo de vacíos temporales en la aplicación del Reglamento.

3.2.3. Derogación de normas

La disposición derogatoria única establece la derogación de cuantas disposiciones de igual o inferior rango se opongan a lo previsto en el real decreto.

4. ADECUACIÓN DEL PROYECTO AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

4.1. Título competencial prevalente

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 Española, que atribuyen al Estado la competencia exclusiva sobre:

- Comercio exterior (10.ª), en la medida en que la norma se inserta en el marco del mercado interior y de la libre circulación de productos armonizados en la Unión Europea.
- Bases y coordinación de la planificación general de la actividad económica (13.ª), por su incidencia en un sector transversal como el de los productos con elementos digitales y la ciberseguridad asociada a los mismos.
- Telecomunicaciones (21.ª), dado que buena parte de los productos afectados se integran en redes y servicios de comunicaciones electrónicas, y la autoridad de vigilancia del mercado designada se encuadra en el Ministerio competente en dicha materia.
- Seguridad pública (29.ª), en cuanto la ciberseguridad de productos digitales se conecta directamente con la protección de infraestructuras críticas, servicios esenciales y otros activos de interés para la seguridad nacional.

El contenido del proyecto de real decreto —designación de autoridades de vigilancia del mercado y notificante, articulación de mecanismos de cooperación y uso de capacidades técnicas estatales— se sitúa plenamente en el ámbito de estas competencias exclusivas del Estado.

De acuerdo con las mencionadas competencias estatales, el proyecto procede a:

- La designación de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID) como autoridad de vigilancia del mercado a efectos del CRA, en la línea con otros ámbitos de productos digitales y ciberseguridad (por ejemplo, el Reglamento Delegado (UE) 2022/30 sobre requisitos de ciberseguridad para determinados equipos radioeléctricos o la normativa proyectada en materia de inteligencia artificial).
- La designación del Centro Criptológico Nacional (CCN) como autoridad notificante, coherente con su estatuto como Autoridad Nacional de Certificación de la Ciberseguridad al amparo del Reglamento (UE) 2019/881 y el Real Decreto 421/2004.
- La designación de INCIBE como laboratorio de apoyo técnico preferente, sin facultades decisorias, y la articulación de su colaboración con la SETID y ENAC.
- La creación de una Comisión de coordinación del Reglamento de Ciberresiliencia, integrada por órganos de la AGE, para la cooperación entre autoridad de vigilancia del mercado y autoridad notificante.
- La articulación de la cooperación con la oficina de enlace única ya designada en virtud del Real Decreto 209/2024.

Por tanto, la norma no regula aspectos propios de la organización o la prestación de servicios de competencia autonómica o local (por ejemplo, consumo, comercio interior o industria en su dimensión no armonizada), sino que se limita a organizar cómo el Estado cumple las obligaciones que el Derecho de la Unión impone a España como Estado miembro en materia de vigilancia del mercado y notificación.

5. DESCRIPCIÓN DE LA TRAMITACIÓN

5.1. Informes y dictámenes

En el curso de la tramitación del proyecto de real decreto se han de recabar, de conformidad con la Ley 50/1997, de 27 de noviembre, del Gobierno:

- Informes de los Ministerios afectados por razón de la materia, en particular:
  - Ministerio de Defensa (por el papel del Centro Criptológico Nacional como autoridad notificante y autoridad nacional de certificación de la ciberseguridad).
  - Ministerios con competencias en economía, industria, comercio, consumo y transformación digital, en la medida en que participan en el sistema nacional de vigilancia del mercado de productos.
- Informe de la Agencia Española de Protección de Datos, habida cuenta de que el Reglamento de Ciberresiliencia y su aplicación interna inciden en la seguridad de tratamientos de datos personales realizados mediante productos con elementos digitales.
- Informe de la Oficina de Coordinación y Calidad Normativa (OC&CN), de acuerdo con el artículo 26.9 de la Ley 50/1997 y el propio Real Decreto 931/2017, sobre la adecuación del proyecto a los principios de buena regulación y a la planificación normativa.
- Informe de la Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública, en cuanto departamento proponente, sobre la corrección técnica y la adecuación del texto al ordenamiento jurídico.

Asimismo, debe recabarse la aprobación previa del Ministerio de Hacienda (art. 26.5. de la Ley 50/1997).

Finalmente, dado el carácter reglamentario de la iniciativa y su conexión directa con la ejecución del Derecho de la Unión Europea, está prevista la solicitud de dictamen del Consejo de Estado, de conformidad con su Ley Orgánica y el artículo 22 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

5.2. Participación pública

5.2.1. Consulta pública previa

De acuerdo con el artículo 133.1 de la Ley 39/2015, de 1 de octubre, y con el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, e**l** proyecto ha sido sometido a un trámite de consulta pública realizado en la sede electrónica del MTDFP desde el día 1 de diciembre de 2025 hasta el día 17 de diciembre de 2025.

Se han **presentado aportaciones por Telefónica y fundación Esys.**

5.2.2. Trámite de audiencia e información pública

De acuerdo con el artículo 133.2 de la Ley 39/2015, de 1 de octubre, y con el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, el proyecto debe someterse a un trámite de audiencia e información pública a realizar a través de la sede electrónica del MTDFP.

6. ANÁLISIS DE IMPACTOS

6.1. Consideraciones generales

El análisis de impacto económico de este proyecto de real decreto parte de un escenario de referencia en el que el Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia o "**CRA") ya es plenamente aplicable** y ha impuesto directamente a los operadores económicos y a los Estados miembros el conjunto de obligaciones materiales en materia de ciberseguridad de los productos con elementos digitales.

En este contexto, **el proyecto de real decreto no introduce requisitos técnicos adicionales ni nuevas obligaciones de fondo** para fabricantes, importadores, distribuidores u otros operadores económicos, más allá de las previstas directamente en el CRA.

6.2. Impacto económico

6.2.1. Efectos sobre la economía en general y los sectores afectados

El impacto económico de la iniciativa es muy limitado dado alcance de la iniciativa, que se limita a designar autoridades competentes y a articular mecanismos internos de coordinación para la aplicación del Reglamento de Ciberresiliencia, lo que aporta seguridad jurídica y previsibilidad a los fabricantes, importadores y distribuidores de productos con elementos digitales sin introducir requisitos técnicos adicionales ni nuevas obligaciones materiales para los operadores económicos más allá de las que impone directamente el Reglamento de Ciberresiliencia.

6.2.2. Efectos sobre la competencia

El proyecto de real decreto se limita a operativizar en España el marco común establecido por el Reglamento de Ciberresiliencia, sin introducir requisitos técnicos nacionales adicionales, imponer esquemas de certificación nacionales obligatorios ni favorecer a tipos concretos de operadores

Por tanto, el impacto del proyecto real decreto sobre la competencia puede calificarse como neutro, con un posible efecto ligeramente positivo al reforzar la igualdad de condiciones en la aplicación nacional del mismo marco europeo para todos los operadores.

6.2.3. Efectos sobre la unidad de mercado

El proyecto normativo es conforme con los principios de la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado.

6.2.4. Test PYME (impacto sobre pymes y microempresas)

El impacto incremental sobre pymes y microempresas se estima prácticamente nulo, por varias razones:

- el proyecto de real decreto no genera nuevas cargas específicas ni diferenciadas para las pymes más allá de las inherentes al CRA;
- se prevén únicamente actuaciones de información/orientación a PYMES con medios existentes, sin derechos subjetivos ni coste adicional;
- contribuye indirectamente a que las pymes se beneficien de un entorno normativo más estable, previsible y coherente en la aplicación del CRA, lo cual facilita la planificación de inversiones en ciberseguridad y el acceso a mercados de otros Estados miembros;

Por ello, el impacto del real decreto sobre pymes y microempresas en España se considera neutro en términos de cargas y ligeramente positivo en términos de seguridad jurídica y entorno competitivo.

6.3. Impacto presupuestario

La aplicación del Reglamento de Ciberresiliencia exige que las autoridades de vigilancia del mercado, la autoridad notificante y los organismos de apoyo técnico dispongan de capacidades personales, materiales y de laboratorio suficientes.

Al respecto hay que tener en cuenta que:

- Las obligaciones de vigilancia de mercado, de disponibilidad de capacidades técnicas, de evaluación y supervisión de organismos de evaluación de la conformidad y de coordinación europea ya vienen impuestas directamente por el CRA.

- El proyecto de norma se limita a determinar qué órganos y entidades ya existentes (SETID, CCN, INCIBE, ENAC, CSIRT coordinador) asumirán las funciones exigidas por el CRA y cómo se coordinan entre sí, sin crear nuevas obligaciones materiales ni exigir actuaciones adicionales más allá de las ya previstas en el Reglamento europeo; así:
  - ✓ La SETID ya actúa como autoridad de vigilancia del mercado en el ámbito de las telecomunicaciones y equipos radioeléctricos.
  - ✓ El CCN ya desempeña funciones equivalentes a las de autoridad notificante como Autoridad Nacional de Certificación de la Ciberseguridad.
  - ✓ INCIBE ya dispone de laboratorio de ciberseguridad y personal especializado.
- La gran parte de las capacidades necesarias ya se financia y despliega en España en el marco de la vigilancia de mercado RED y del Reglamento Delegado (UE) 2022/30 (RED-DA), cuya ciberseguridad se integra en el CRA a partir de su plena aplicabilidad y de la derogación prevista del RED-DA desde el 11 de diciembre de 2027
- Las necesidades de adaptación (formación, ajustes de sistemas de información, intensificación de ensayos) se abordan reordenando y priorizando créditos de los programas presupuestarios ya existentes de la SETID, del CCN y de INCIBE.

En consecuencia, el impacto presupuestario atribuible específicamente al proyecto de real decreto puede calificarse como nulo o, en todo caso, absorbible con los recursos humanos existentes, en la medida en que:

- No implica creación de nuevas estructuras administrativas.
- No comporta incrementos de plantilla vinculados exclusivamente a la norma.
- No requiere ampliaciones de crédito adicionales a las ya previstas para la aplicación del CRA en su conjunto.
- Se basa en la reasignación y compensación interna de recursos dentro de un sistema de vigilancia de mercado y certificación de ciberseguridad que ya existe y que se adapta al nuevo marco europeo.

En definitiva, el proyecto procede a la reasignación de medios ya existentes (SETID, CCN, INCIBE y apoyo contractual), sin creación de estructuras administrativas ex novo ni incremento de dotaciones ligado a la norma, sin perjuicio de las decisiones presupuestarias futuras que, en su caso, requiera el cumplimiento global del CRA.

6.4. Análisis de cargas administrativas

En cuanto a las cargas administrativas – entendidas como “aquellas actividades de naturaleza administrativa que deben llevar a cabo las empresas y ciudadanos para cumplir con las obligaciones derivadas de la normativa”-, no se derivan del proyecto de real decreto.

El proyecto normativo no introduce nuevas obligaciones de información, comunicación o tramitación para los operadores económicos ni para la ciudadanía respecto de las ya previstas directamente en el Reglamento de Ciberresiliencia. Las eventuales cargas administrativas (notificación de incidentes, aportación de documentación técnica, etc.) derivan del propio Reglamento CRA y no del proyecto normativo, que se limita a designar autoridades y articular mecanismos internos de coordinación.

Por ello, el impacto del real decreto sobre las cargas administrativas se considera **nulo.**

6.5. Impacto por razón de género

A los efectos de lo previsto en el artículo 19 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres y el artículo 26.3.f) de la Ley 50/1997, de 27 de noviembre, del Gobierno, se señala que el proyecto tiene un impacto de género **nulo** en esta materia.

6.6. Impacto en infancia, adolescencia y familia.

De conformidad con lo dispuesto en el artículo 22 quinquies de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, en la redacción dada por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, y en el artículo 2.1.f) del Real Decreto 931/2017, de 27 de octubre, el proyecto normativo tiene un impacto **nulo** en esta materia.

De acuerdo con lo previsto en la disposición adicional décima de la Ley 40/2003, de 18 de noviembre, de protección a las familias numerosas, introducida por la disposición final quinta de la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, el contenido del proyecto tiene un impacto **nulo** en la familia.

6.7. Impacto en materia de protección de datos personales

El ámbito material del Reglamento de Ciberresiliencia abarca productos con elementos digitales que, en una proporción muy significativa, tratan datos personales, incluidos datos de uso, de comportamiento y, en algunos casos, categorías especiales de datos.

El Reglamento de Ciberresiliencia:

- exige que los productos se diseñen, desarrollen y produzcan con arreglo a principios de ciberseguridad desde el diseño y por defecto,
- impone obligaciones de gestión de vulnerabilidades y de actualización de seguridad durante la vida útil del producto,

- y refuerza la responsabilidad de fabricantes e importadores en relación con la prevención de accesos no autorizados, manipulaciones maliciosas y otros incidentes que pueden derivar en violaciones de seguridad de los datos personales.

Estas obligaciones son complementarias de las establecidas en el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, en particular en lo relativo a la seguridad del tratamiento (artículo 32 RGPD) y la protección de datos desde el diseño y por defecto (artículo 25 RGPD).

El proyecto de real decreto contribuye a que estos objetivos se cumplan de forma más eficaz al:

- designar de forma clara a la autoridad de vigilancia del mercado y a la autoridad notificante para productos con elementos digitales,
- dotar a dichas autoridades de un laboratorio técnico de apoyo preferente, capaz de verificar el cumplimiento de los requisitos de ciberseguridad,
- y articular mecanismos de coordinación que facilitan la detección y respuesta ante productos inseguros o con vulnerabilidades explotadas, reduciendo el riesgo de brechas de datos personales.

Desde el punto de vista del tratamiento de datos por parte de las autoridades:

- el real decreto no crea nuevas bases de datos ni registros específicos de carácter personal, más allá de los inherentes a la gestión de expedientes de vigilancia de mercado, que ya se encuentran amparados en la normativa sectorial y general de procedimiento administrativo;
- cualquier tratamiento de datos personales que las autoridades realicen en la aplicación del real decreto deberá estar sometido a las garantías del RGPD y de la Ley Orgánica 3/2018 (principios de licitud, minimización, limitación de la finalidad, plazos de conservación, deber de secreto, etc.).

En este marco, el impacto del real decreto en materia de protección de datos personales se califica como positivo, en la medida en que:

- refuerza la capacidad del sector público para detectar y corregir vulnerabilidades que podrían afectar a la confidencialidad, integridad y disponibilidad de datos personales,
- favorece, de forma indirecta, la aplicación efectiva de los principios de seguridad y minimización de datos en el diseño y funcionamiento de productos con elementos digitales,
- y no introduce nuevos riesgos significativos para la protección de datos, siempre que los tratamientos que realicen las autoridades se ajusten a la normativa vigente.

6.8. Otros impactos considerados

6.8.1. Impacto medioambiental y por razón de cambio climático

El real decreto tiene un contenido estrictamente organizativo en materia de designación de autoridades y coordinación administrativa.

No regula el consumo energético de los productos, su ciclo de vida material ni aspectos relacionados con residuos electrónicos, emisiones o huella de carbono.

En este sentido no se identifican impactos ambientales directos atribuibles a la norma, ni efectos significativos sobre las políticas de cambio climático.

De forma muy indirecta, podría considerarse que una mejor gestión de vulnerabilidades y actualizaciones de seguridad puede alargar la vida útil de ciertos dispositivos digitales, reduciendo la necesidad de sustitución prematura y, por tanto, los residuos electrónicos asociados. No obstante, estos posibles efectos son difíciles de cuantificar y dependen fundamentalmente de la aplicación del Reglamento de Ciberresiliencia por parte de los fabricantes, no del contenido de este real decreto.

Por ello, el impacto ambiental específico del real decreto se califica como nulo o, en todo caso, marginal.

6.8.2. Impacto en igualdad de oportunidades, no discriminación y accesibilidad

El impacto específico del real decreto en materia de igualdad de oportunidades, no discriminación y accesibilidad se considera nulo.

6.8.3. Otros impactos relevantes (sociales, tecnológicos, etc.)

Aunque el real decreto no introduce obligaciones materiales nuevas para los operadores económicos, su contribución a la organización del sistema de supervisión CRA sí tiene algunos impactos cualitativos de carácter social y tecnológico:

6.8.3.1. Impacto social y en la confianza digital:

Al clarificar qué autoridades son competentes para vigilar el mercado de productos con elementos digitales y al dotarlas de un laboratorio de apoyo, se favorece una aplicación más efectiva y coherente del Reglamento de Ciberresiliencia, lo que puede aumentar la confianza de ciudadanos y empresas en la seguridad de los productos digitales.

Este efecto es difícil de cuantificar, pero es relevante en un contexto de creciente dependencia de servicios y dispositivos conectados.

6.8.3.2. Impacto tecnológico e industrial:

La existencia de una autoridad de vigilancia de mercado y de una autoridad notificante claramente identificadas, junto con un laboratorio de apoyo especializado, puede incentivar que los fabricantes e

importadores adopten prácticas de ciberseguridad desde el diseño y busquen soluciones técnicas de mayor calidad, reforzando el tejido industrial de ciberseguridad.

Asimismo, la experiencia acumulada por las autoridades en la evaluación de productos con elementos digitales puede trasladarse a mejores guías, recomendaciones y buenas prácticas para el mercado.

Estos impactos, aunque positivos, están intrínsecamente ligados al despliegue del Reglamento de Ciberresiliencia como norma europea. El real decreto contribuye a que dichos efectos se produzcan de forma más ordenada y eficiente, pero no los genera por sí mismo, por lo que su carácter es principalmente instrumental y difícil de aislar cuantitativamente.

7. EVALUACIÓN "EX POST"

No se considera necesaria llevar a cabo una evaluación ex post, ya que la norma prácticamente se limita a asignar responsabilidades y funciones entre distintas autoridades administrativas.