C/2026/6013

17.11.2026

COMUNICACIÓN DE LA COMISIÓN

Orientaciones de la Comisión sobre la aplicación del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia)

(C/2026/6013)

Índice

Página

1. INTRODUCCIÓN 3
   - 1.1. El Reglamento de Ciberresiliencia 3
   - 1.2. Objeto de estas orientaciones 3
2. ÁMBITO DE APLICACIÓN 4
   - 2.1. Introducción en el mercado 4
   - 2.2. Programas informáticos como productos con elementos digitales 5
   - 2.3. Código informático 6
   - 2.4. Combinación de equipos informáticos y programas informáticos que forman un producto con elementos digitales 7
   - 2.5. Conexión de datos 8
   - 2.6. Sistemas complejos 8
   - 2.7. Productos con elementos digitales diseñados antes de la fecha de aplicación del Reglamento de Ciberresiliencia 9
3. PROGRAMAS INFORMÁTICOS LIBRES Y DE CÓDIGO ABIERTO 11
   - 3.1. Determinación de cuándo un programa informático libre y de código abierto se considera responsabilidad de una persona 12
   - 3.2. Determinación de cuándo un programa informático libre y de código abierto se introduce en el mercado de la UE 13
     - 3.2.1. Cobro de un precio 13
     - 3.2.2. Monetización de otros servicios o exigencia del tratamiento de datos personales 13
     - 3.2.3. Servicios de asistencia 14
     - 3.2.4. Donaciones 15
     - 3.2.5. Financiación de programas informáticos libres y de código abierto 15
     - 3.2.6. Entidades sin ánimo de lucro constituidas para alcanzar objetivos sin ánimo de lucro 16
     - 3.2.7. Integración por parte de otros fabricantes 16
   - 3.3. Administradores de comunidad de programas informáticos de código abierto 16
     - 3.3.1. Apoyo continuado y garantía de la viabilidad del programa informático libre y de código abierto 17
   - 3.4. Colaboradores y usos *downstream* 18
   - 3.5. Ejemplos ilustrativos 19
4. MODIFICACIONES SUSTANCIALES Y PIEZAS DE RECAMBIO 21
   - 4.1. Reparaciones físicas 22
   - 4.2. Piezas de recambio 23
   - 4.3. Actualizaciones de programas informáticos como modificaciones sustanciales 24

4.4. Consecuencias de una modificación sustancial 27
4.4.1. Modificaciones sustanciales realizadas por una persona distinta del fabricante original 28
4.4.2. Modificaciones sustanciales realizadas por el fabricante original 29
5. PERÍODO DE SOPORTE 29
5.1. Modificaciones sustanciales y período de soporte 31
6. PRODUCTOS IMPORTANTES Y CRÍTICOS CON ELEMENTOS DIGITALES 32
6.1. Funcionalidad principal 33
6.2. Evaluación de la conformidad para productos importantes y críticos con elementos digitales 36
6.3. Implicaciones para la presunción de conformidad 38
7. EVALUACIÓN DE LOS RIESGOS DE CIBERSEGURIDAD E INTEGRACIÓN DE PRODUCTOS CON ELEMENTOS Y COMPONENTES DIGITALES 41
7.1. Sobre la evaluación y el tratamiento de los riesgos de ciberseguridad 41
7.2. Sobre el diseño, el desarrollo y la producción de productos con elementos digitales de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes 42
7.3. Evaluación de riesgos y diligencia debida en relación con las dependencias externas y los componentes integrados 42
7.4. Reutilización de las evaluaciones de riesgos y la documentación de conformidad para familias de productos con elementos digitales 44
8. TRATAMIENTO DE DATOS A DISTANCIA 44
8.1. ¿Qué se considera una solución de tratamiento de datos a distancia para un producto con elementos digitales? 45
8.1.1. La noción de «a distancia» 46
8.1.2. La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones? 46
8.1.3. El programa informático ¿ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad? 47
8.2. Implicaciones prácticas y técnicas de las soluciones de tratamiento de datos a distancia y dependencia de soluciones de terceros 49
8.3. Casos de uso de soluciones de tratamiento de datos a distancia 50
8.3.1. Aplicación de banca móvil 51
8.3.2. Termostato inteligente 52
8.3.3. Lector de libros electrónicos 53
8.3.4. Robot industrial 53
8.3.5. Red de telefonía celular 53
9. ELEMENTOS ADICIONALES 54
9.1. Obligaciones de información 54
9.2. Gestión de las vulnerabilidades 56
9.2.1. Notificación *upstream* y puesta en común de las correcciones de seguridad 56
9.2.2. Vulnerabilidades aprovechables conocidas 57
9.2.3. Exámenes y pruebas eficaces y periódicos 58
9.3. Coherencia con otros actos legislativos 59
9.3.1. Reglamento (UE) 2019/2144 y Reglamento (UE) n.º 168/2013 59
9.3.2. Validez de los certificados de examen de tipo UE (artículo 69, apartado 1) 59

1. **INTRODUCCIÓN**

1.1. **El Reglamento de Ciberresiliencia**

1. 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]) entró en vigor el 10 de diciembre de 2024. El Reglamento tiene por objeto reforzar el enfoque de la Unión respecto a la ciberseguridad, abordar la ciberresiliencia a escala de la UE y mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la introducción de productos con elementos digitales en el mercado la UE, así como durante el ciclo de vida de los productos con elementos digitales.

2. El Reglamento de Ciberresiliencia se basa en el nuevo marco legislativo de la UE establecido en el 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, y en la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo ([2]).

3. Las autoridades nacionales de vigilancia del mercado se encargan de la vigilancia del mercado y de velar por su cumplimiento. Los productos con elementos digitales que entran en el ámbito de aplicación del Reglamento de Ciberresiliencia están sujetos al 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.º 765/2008 y (UE) n.º 305/2011. La Comisión y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) apoyan a los operadores económicos y a los Estados miembros en la aplicación del Reglamento de Ciberresiliencia.

1.2. **Objeto de estas orientaciones**

4. El artículo 26, apartado 1, del Reglamento de Ciberresiliencia exige que la Comisión publique orientaciones para ayudar a los operadores económicos a aplicar el Reglamento, haciendo especial hincapié en facilitar su cumplimiento por parte de las microempresas y las pequeñas y medianas empresas. El artículo 26, apartado 2, establece los aspectos mínimos que deben abordar las orientaciones. Entre ellos, se incluyen los siguientes: i) el ámbito de aplicación del Reglamento de Ciberresiliencia (en particular, las soluciones de tratamiento de datos a distancia y los programas informáticos libres y de código abierto); ii) el concepto de «períodos de soporte»; iii) la interacción entre el Reglamento de Ciberresiliencia y otros actos legislativos de la UE; y iv) el concepto de «modificación sustancial».

5. El 3 de diciembre de 2025, la Comisión publicó una serie de preguntas frecuentes destinadas a ayudar a los operadores económicos a prepararse para la aplicación del Reglamento de Ciberresiliencia ([3]).

6. Las presentes orientaciones tienen por objeto ayudar a los operadores económicos a cumplir el Reglamento de Ciberresiliencia y apoyar las actividades de las autoridades de vigilancia del mercado, las autoridades notificantes y los organismos notificados, con el fin de garantizar una aplicación armonizada del Reglamento en toda la Unión. Estas orientaciones no pretenden abarcar el Reglamento de Ciberresiliencia en todo su ámbito de aplicación, sino proporcionar aclaraciones sobre la justificación de determinadas disposiciones clave y cómo podrían aplicarse en la práctica. Las orientaciones se refieren al Reglamento de Ciberresiliencia y no son aplicables a otros actos legislativos de la UE.

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

([2]) El programa de trabajo de la Comisión para 2026 prevé la presentación de una «Ley Europea de Productos» que actualice el nuevo marco legislativo y las normas sobre vigilancia del mercado y estandarización: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52025DC0870.

([3]) Las preguntas frecuentes pueden descargarse a través del sitio web de aplicación del Reglamento de Ciberresiliencia de la Comisión, desde la página web específica de preguntas frecuentes.

7. En la preparación de las presentes orientaciones se consultó ampliamente a las partes interesadas, en particular al Grupo de Expertos sobre ciberseguridad de los productos con elementos digitales ([4]) y a través de una consulta pública que se celebró entre el 3 de marzo y el 13 de abril de 2026 ([5]).

8. Las presentes orientaciones no son vinculantes para los operadores económicos u otros agentes sujetos al Reglamento de Ciberresiliencia. Solo el Tribunal de Justicia de la Unión Europea (TJUE) puede ofrecer una interpretación autorizada del Reglamento de Ciberresiliencia. No obstante, estas orientaciones exponen la interpretación que hace la Comisión del Reglamento de Ciberresiliencia, con el fin de apoyar su cumplimiento y contribuir a su aplicación efectiva. Además, las orientaciones contienen varios ejemplos para ilustrar la aplicación de disposiciones específicas. No obstante, estos ejemplos no pretenden sustituir a una evaluación caso por caso, que siempre será necesaria para tener en cuenta las especificidades de cada caso particular.

9. De conformidad con el artículo 26 del Reglamento de Ciberresiliencia, la Comisión puede considerar la posibilidad de elaborar orientaciones adicionales, entre ellas orientaciones dirigidas a los fabricantes sujetos al Reglamento y a otra legislación de armonización de la Unión o a otros actos jurídicos conexos de la Unión. Por ejemplo, estas orientaciones pueden abordar cuestiones relativas a la interacción entre el Reglamento de Ciberresiliencia y el Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial), y el Reglamento (UE) 2022/2554, sobre la resiliencia operativa digital del sector financiero.

2. ÁMBITO DE APLICACIÓN

2.1. Introducción en el mercado

10. El Reglamento de Ciberresiliencia se aplica a los productos con elementos digitales que se comercializan en el mercado de la UE. El concepto de «comercialización» se define en el artículo 3, punto 22, del Reglamento como «el suministro, ya sea remunerado o gratuito, de un producto con elementos digitales para su distribución o utilización en el mercado de la Unión en el curso de una actividad comercial». De conformidad con el artículo 3, punto 21, un producto con elementos digitales se introduce en el mercado de la UE la primera vez que se comercializa.

11. La última edición de la «Guía azul» sobre la aplicación de la normativa europea relativa a los productos, publicada en 2022 (en lo sucesivo, «la Guía azul») ([6]), ofrece orientaciones que facilitan la comprensión de las normas de la UE relativas a los productos y su aplicación uniforme en los diferentes marcos jurídicos sectoriales adaptados al nuevo marco legislativo, como el Reglamento de Ciberresiliencia. La Guía azul indica que los conceptos de «introducción en el mercado» y de «comercialización» deben entenderse en el sentido de que se refieren a «un producto individual y no a un tipo de producto, y al hecho de si el producto ha sido fabricado de manera individual o en serie» (sección 2.3).

12. En el caso de los productos más «tradicionales» con elementos digitales cubiertos por el nuevo marco legislativo, como los equipos informáticos en forma de máquinas o los productos de equipos radioeléctricos con elementos digitales, el concepto de «introducción en el mercado» está bien establecido, y la Guía azul ofrece orientaciones adicionales para aclarar en qué momento se considera que dichos productos han sido introducidos en el mercado. Los «ejemplos de resumen» que figuran en la sección 2.12 de la Guía azul ofrecen otros ejemplos del concepto de «introducción en el mercado».

13. No obstante, dada la naturaleza de los productos intangibles con elementos digitales, como los programas informáticos autónomos, es necesario proporcionar orientaciones adicionales sobre el momento en que se considera que dichos productos con elementos digitales han sido introducidos en el mercado. Una vez completada la fase de fabricación del programa informático y una vez que el producto con elementos digitales se ha ofrecido a los posibles usuarios en el mercado de la UE, puede considerarse que su fabricante ha producido múltiples copias del mismo producto con elementos digitales consistente en un programa informático y las ha suministrado para su distribución o uso. De hecho, a diferencia de los productos tangibles con elementos digitales, los programas

([4]) Grupo de Expertos sobre ciberseguridad de los productos con elementos digitales en el registro de grupos de expertos de la Comisión y otras entidades similares.
([5]) Consulta pública sobre el proyecto de orientaciones de la Comisión relativas al Reglamento de Ciberresiliencia.
([6]) Comunicación de la Comisión titulada «"Guía azul" sobre la aplicación de la normativa europea relativa a los productos, de 2022»2022/C 247/01 (DO C 247 de 29.6.2022, p. 1).

informáticos autónomos no están sujetos a limitaciones físicas de producción o de existencias: cada vez que el programa informático se pone a disposición para su descarga o distribución se crea una nueva copia idéntica para el usuario. Siempre que esa versión del programa informático no se modifique de manera que afecte al cumplimiento del Reglamento de Ciberresiliencia, se considerará que la introducción en el mercado de la UE se ha producido en el momento en que se ofrece por primera vez para su distribución o uso. Por lo tanto, la posibilidad de descargar o distribuir posteriormente esa versión del producto con elementos digitales consistente en un programa informático debe considerarse un caso de puesta a disposición de dicho producto con elementos digitales ([7]).

14. Por lo tanto, debe considerarse que un producto con elementos digitales consistente en un programa informático autónomo se ha introducido en el mercado cuando se haya completado su fase de fabricación y dicho programa informático se suministre por primera vez para su distribución o uso en el mercado de la UE en el transcurso de una actividad comercial. Debe considerarse que el fabricante ha introducido en el mercado al mismo tiempo múltiples copias del mismo producto con elementos digitales consistente en un programa informático. Por lo tanto, aunque múltiples copias del mismo programa informático siguen siendo productos individuales con elementos digitales, se considera que se han introducido en el mercado al mismo tiempo, con independencia del momento en que la posesión o el uso de cada copia individual se transfiera a otra persona física o jurídica. Al mismo tiempo, cuando el fabricante comercializa programas informáticos en diversas variantes que difieren en los componentes que incluyen, las configuraciones o las funcionalidades habilitadas (por ejemplo, versiones para distintos sistemas operativos o paquetes con diferentes conjuntos de funcionalidades), dichas variantes no pueden considerarse múltiples copias del mismo producto con elementos digitales consistente en un programa informático. Por lo tanto, deben tratarse como productos distintos con elementos digitales a efectos de su introducción en el mercado.

Ejemplo1: el 1 de enero de 2028, la empresa A suministra por primera vez la versión 1.0.0 de su programa informático X para su distribución a través de su sitio web. El mismo día, el cliente 1 compra una copia de la versión 1.0.0 del programa informático X. El 15 de enero de 2028, el cliente 2 compra una copia de la versión 1.0.0 del programa informático X. Ambas copias de la versión 1.0.0 del programa informático X se introducen en el mercado el 1 de enero de 2028.

15. Dado el carácter iterativo del desarrollo de programas informáticos, debe aclararse además que las iteraciones posteriores de un producto con elementos digitales consistente en un programa informático se consideran una nueva introducción en el mercado cuando dichas iteraciones constituyen una «modificación sustancial» de un producto con elementos digitales consistente en un programa informático ya introducido en el mercado, como se indica en el considerando 41 del Reglamento de Ciberresiliencia. Las iteraciones que no constituyan modificaciones sustanciales no obligan al fabricante a realizar un nuevo procedimiento de evaluación de la conformidad y, por tanto, no modifican la fecha de introducción en el mercado de dicho programa informático. Para más información sobre el concepto de «modificación sustancial», véase la sección 4 Modificaciones sustanciales y piezas de recambio.

Ejemplo 2: el 1 de enero de 2028, la empresa A suministra por primera vez la versión 1.0.0 de su programa informático X para su distribución a través de su sitio web. El mismo día, el cliente 1 compra una copia de la versión 1.0.0 del programa informático X. El 15 de enero de 2028, la empresa A publica una versión actualizada, la versión 1.0.1, del programa informático X que no constituye una modificación sustancial. El 30 de enero de 2028, el cliente 2 compra una copia de la versión 1.0.1 del programa informático X. Se considera que ambas copias de las versiones 1.0.0 y 1.0.1 del programa informático X se introdujeron en el mercado el 1 de enero de 2028.

16. Las orientaciones establecidas en los puntos 13, 14 y 15 se aplican exclusivamente en la medida en que el producto con elementos digitales sea un programa informático autónomo. No es así, por ejemplo, cuando el programa informático se combina con un equipo informático, como se expone en la sección *2.4* Combinación de equipos informáticos y programas informáticos que forman un producto con elementos digitales.

2.2. **Programas informáticos como productos con elementos digitales**

17. El artículo 3, punto 1, del Reglamento de Ciberresiliencia define un producto con elementos digitales como un «producto consistente en programas informáticos o equipos informáticos y sus soluciones de tratamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado». Dichos productos con elementos digitales entran en el ámbito de aplicación del Reglamento de Ciberresiliencia cuando su finalidad prevista o su uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

([7]) De conformidad con el artículo 13, apartado 11, los fabricantes podrán mantener archivos públicos de programas informáticos que mejoren el acceso de los usuarios a las versiones históricas. En tales casos, se informará claramente y de manera fácilmente accesible a los usuarios sobre los riesgos asociados al uso de programas informáticos a los que no se da soporte.

18. Por tanto, el Reglamento de Ciberresiliencia puede aplicarse a una gama de productos con elementos digitales, entre ellos: i) programas informáticos autónomos, como aplicaciones y programas de ordenador, tanto si se distribuyen por medios digitales como físicos; ii) equipos informáticos con programas informáticos incorporados (por ejemplo, dispositivos de internet de las cosas, ordenadores portátiles y tabletas); iii) equipos informáticos autónomos (por ejemplo, circuitos integrados y placas madre); y iv) cualquier combinación de equipos informáticos y programas informáticos suministrados por separado, pero destinados a funcionar conjuntamente.

19. Por lo tanto, los programas informáticos autónomos entran en el ámbito de aplicación del Reglamento de Ciberresiliencia cuando se introducen en el mercado como productos con elementos digitales. Conviene distinguir entre los productos con elementos digitales consistentes en programas informáticos que están sujetos al Reglamento de Ciberresiliencia y la prestación a distancia de servicios que no entran en el ámbito de aplicación del Reglamento.

20. Para que un programa informático entre en el ámbito de aplicación del Reglamento de Ciberresiliencia, el producto con elementos digitales consistente en un programa informático debe proporcionarse a un usuario, debe obtenerlo dicho usuario y debe ejecutarse en un sistema electrónico de información del usuario o como parte de este. Los programas informáticos que se descargan, instalan o suministran de otro modo al usuario y que se ejecutan en el sistema electrónico de información del usuario cumplen estos criterios, por ejemplo, cuando adoptan la forma de una extensión del navegador o de una aplicación desarrollada utilizando tecnologías web, pero suministrada para su ejecución local.

21. En cambio, los programas informáticos que se ejecutan a distancia y a los que el usuario simplemente accede no constituyen, por ese mero hecho, productos con elementos digitales. Recitals 11 and 12 of the CRA, in fact, draw this distinction, by explaining that processing or storage at a distance is subject to the CRA only to the extent that it is necessary for a product with digital elements to perform its functions (i.e. through the concept of remote data processing as defined in Article 3(2)), and not itself as a product with digital elements. Este suele ser el caso de las aplicaciones web, incluidas las aplicaciones web progresivas, a las que se accede exclusivamente a través de un navegador web. Lo mismo ocurre con los sitios web: aunque, desde un punto de vista técnico, los sitios web puedan ejecutarse y funcionar en cierta medida en el dispositivo del usuario, del considerando 12 del Reglamento de Ciberresiliencia se desprende que los sitios web no deben considerarse por sí mismos productos con elementos digitales y que solo entran en el ámbito de aplicación del Reglamento cuando admiten la funcionalidad de un producto con elementos digitales, es decir, en la medida en que constituyan un tratamiento de datos a distancia (como se explica con más detalle en la sección *8* y, en particular, en *8.1.2* La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones?).

Ejemplo 3: una aplicación móvil que un usuario descarga de una tienda de aplicaciones y que instala en su teléfono inteligente se suministra al usuario y se ejecuta en el dispositivo del usuario, por lo que constituye un producto con elementos digitales. Cuando se introduce en el mercado en el transcurso de una actividad comercial, puede entrar en el ámbito de aplicación del Reglamento de Ciberresiliencia.

Ejemplo 4: una aplicación de escritorio desarrollada utilizando tecnologías web, pero empaquetada para su instalación local, se suministra al usuario y se ejecuta en el dispositivo del usuario, por lo que constituye un producto con elementos digitales. Cuando se introduce en el mercado en el transcurso de una actividad comercial, puede entrar en el ámbito de aplicación del Reglamento de Ciberresiliencia.

Ejemplo 5: una aplicación web a la que el usuario accede exclusivamente a través de un navegador web no es un producto con elementos digitales. A menos que admita la funcionalidad de un producto con elementos digitales, no entra en el ámbito de aplicación del Reglamento de Ciberresiliencia. En cambio, una aplicación suministrada al usuario como cliente instalado localmente que se ejecuta en el dispositivo del usuario sí constituye un producto con elementos digitales. Cuando se introduce en el mercado en el transcurso de una actividad comercial, puede entrar en el ámbito de aplicación del Reglamento de Ciberresiliencia.

Si dicho cliente depende, para desempeñar una o varias de sus funciones, de un tratamiento de datos a distancia que responda a la definición de «tratamiento de datos a distancia», dicho tratamiento también forma parte del producto con elementos digitales.

Ejemplo 6: un sitio web que se limita a presentar información a sus visitantes y no admite la funcionalidad de un producto con elementos digitales no constituye en sí mismo un producto con elementos digitales. Por lo tanto, no entra en el ámbito de aplicación del Reglamento de Ciberresiliencia.

2.3. **Código informático**

22. También conviene aclarar si el código fuente puede constituir un producto con elementos digitales consistente en un programa informático. El Reglamento de Ciberresiliencia define los programas informáticos como «la parte de un sistema electrónico de información consistente en un código informático» (artículo 3, punto 4). El código informático puede adoptar la forma de i) código máquina, que es el conjunto de instrucciones, escritas en formato binario, que el procesador de un ordenador ejecuta directamente; o ii) código fuente, es decir, el conjunto de instrucciones y sentencias escritas en un lenguaje de programación, que deben compilarse o interpretarse para que un ordenador pueda ejecutarlas. La definición de programa informático que establece el Reglamento de Ciberresiliencia abarca ambos tipos de código.

23. Otra cuestión es si un determinado suministro de código informático equivale a la introducción de un producto con elementos digitales en el mercado de la UE, lo que requiere un suministro en el transcurso de una actividad comercial. Este no suele ser el caso del código fuente. Por ejemplo, por lo general no se considera que una persona física o jurídica que comparte código informático libre y de código abierto en repositorios de acceso público esté introduciendo dicho código en el mercado de la UE a efectos del Reglamento de Ciberresiliencia (como se explica detalladamente en la sección 3 Programas informáticos libres y de código abierto). El código sin terminar que se comparte durante la fase de diseño y desarrollo de un producto con elementos digitales (por ejemplo, para realizar pruebas o someterlo a revisión) tampoco se considera que se haya introducido en el mercado a efectos del Reglamento de Ciberresiliencia, ya que su fase de fabricación no ha concluido. Del mismo modo, tampoco se considera que el código de muestra o de demostración proporcionado como parte de tutoriales o material de formación se haya introducido en el mercado a efectos del Reglamento de Ciberresiliencia ([8]).

24. Por otra parte, cuando un fabricante facilita a sus clientes un código informático como producto con elementos digitales, se considera que dicho código se ha introducido en el mercado, con independencia de que se trate de código máquina o de código fuente ([9]).

Ejemplo 7: la empresa A concede a la empresa B una licencia sobre el código fuente para una plataforma interna personalizable y facilita dicho código fuente en un archivo de texto. Aunque la empresa B tenga que adaptar y compilar dicho código fuente antes de utilizarlo, la empresa A introduce ese código fuente en el mercado, por lo que está sujeta al Reglamento de Ciberresiliencia. La empresa A no es responsable de que las posteriores adaptaciones y compilaciones del código realizadas por la empresa B sean conformes con el Reglamento de Ciberresiliencia.

2.4. **Combinación de equipos informáticos y programas informáticos que forman un producto con elementos digitales**

25. El hecho de que un programa informático forme parte de un producto con elementos digitales no debe determinarse en función de cómo o cuándo se entregue dicho programa informático al usuario, sino en función de si, a la luz de la finalidad prevista del producto y de su uso razonablemente previsible, dicho programa informático es necesario para que el producto con elementos digitales realice las funciones previstas. Cuando un producto con elementos digitales consistente en un equipo informático está diseñado para trabajar junto con un programa informático específico suministrado por el mismo fabricante con el fin de realizar sus funciones, el equipo informático y el programa informático constituyen conjuntamente el producto con elementos digitales. Por lo tanto, los programas informáticos necesarios para operar, configurar, controlar o utilizar un producto con elementos digitales de conformidad con su finalidad prevista forman parte del producto con elementos digitales, aun cuando se obtengan a través de un canal independiente (por ejemplo, una tienda de aplicaciones, un enlace de descarga u otro canal digital después de que el producto con elementos digitales consistente en un equipo informático se haya introducido en el mercado). Por lo tanto, su introducción en el mercado se produce en el mismo momento en que se introducen en el mercado las unidades de los productos con elementos digitales consistentes en equipos informáticos.

Ejemplo 8: una impresora de red se introduce en el mercado como producto con elementos digitales consistente en un equipo informático, mientras que los controladores necesarios para enviar trabajos de impresión, configurar el dispositivo y gestionar su funcionamiento se ponen a disposición para su descarga desde el sitio web del fabricante. Aunque la impresora y los controladores se suministran a través de canales diferentes, juntos constituyen un único producto con elementos digitales, ya que la impresora no puede cumplir su finalidad prevista sin los controladores.

Ejemplo 9: un dispositivo ponible para el seguimiento de la actividad física se introduce en el mercado para medir la frecuencia cardíaca y la actividad del usuario, para el cual es necesaria una aplicación para teléfonos inteligentes facilitada por el fabricante a fin de mostrar las mediciones, consultar el historial y configurar el dispositivo. Aunque la aplicación se descarga por separado a través de una tienda de aplicaciones, el dispositivo ponible y la aplicación juntos constituyen un único producto con elementos digitales, ya que están diseñados y destinados a funcionar conjuntamente para proporcionar la funcionalidad del producto con elementos digitales.

([8]) También cabe recordar que el artículo 4, apartado 3, permite que los fabricantes comercialicen programas informáticos inacabados que no sean conformes con el Reglamento, como las versiones alfa, beta o candidatas a lanzamiento, siempre que los programas informáticos inacabados solo estén disponibles durante el tiempo necesario para someterlos a prueba y recabar observaciones.

([9]) Por otra parte, cabe señalar que, a efectos de la legislación sobre la responsabilidad de los productos, el código informático en sí mismo no constituye un producto, por lo que los fabricantes que introducen dicho código en el mercado no pueden ser considerados responsables con arreglo a la Directiva (UE) 2024/2853 (Directiva sobre responsabilidad por los daños causados por productos defectuosos). Recital 13 of that Directive states that «information is not, however, to be considered a product, and product liability rules should therefore not apply to the content of digital files, such as media files or e-books or the mere source code of software». Esto no impide que los fabricantes puedan ser responsables con arreglo al Derecho nacional en materia de responsabilidad civil.

2.5. **Conexión de datos**

26. El artículo 2, apartado 1 establece que el Reglamento de Ciberresiliencia «es aplicable a los productos con elementos digitales comercializados cuya finalidad prevista o uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red». Por lo tanto, el ámbito de aplicación del Reglamento de Ciberresiliencia no se basa en la mera presencia de componentes electrónicos, sino en la capacidad de un producto con elementos digitales para intercambiar información digital.

27. Si bien los términos «conexión lógica» y «conexión física» se definen en el artículo 3, el Reglamento de Ciberresiliencia no define «conexión de datos» ni «datos digitales». Por tanto, conviene establecer una interpretación de lo que es una conexión de datos a fin de aclarar los límites del ámbito de aplicación del Reglamento. Esta delimitación es especialmente importante para distinguir los productos con elementos digitales que se limitan a utilizar señales eléctricas de aquellos que participan en la comunicación digital y, por tanto, están expuestos a riesgos de ciberseguridad.

28. En su nivel más básico, una conexión de datos implica la transmisión de información en forma binaria, es decir, como una secuencia de ceros y unos. El simple hecho de activar y desactivar una salida (es decir, 0/1) no constituye por sí mismo una conexión de datos si dichos estados no están destinados a representar datos o no son leídos por una entrada digital. Para que exista una conexión de datos, los estados binarios deben codificarse deliberadamente como información en un extremo emisor y poder descodificarse como información en el extremo receptor. Es decir, debe haber un emisor que genere deliberadamente símbolos digitales conforme a un esquema definido, así como un receptor capaz de interpretar dichos símbolos como datos. Cuando las señales eléctricas o electrónicas se utilizan únicamente para activar o alimentar una función, sin transmitir información codificada digitalmente, no existe conexión de datos a efectos del Reglamento de Ciberresiliencia y, por tanto, el producto con elementos digitales no entra en el ámbito de aplicación del artículo 2, apartado 1.

2.6. **Sistemas complejos**

29. Los productos con elementos digitales incluidos en el ámbito de aplicación del Reglamento de Ciberresiliencia pueden consistir no solo en dispositivos individuales o componentes de programas informáticos, sino también en sistemas complejos, en particular los sistemas compuestos por múltiples equipos informáticos y programas informáticos que funcionan conjuntamente para desempeñar una determinada función. Cuando dichos sistemas se introducen en el mercado como un único producto con elementos digitales, constituyen un producto con elementos digitales en el sentido del Reglamento de Ciberresiliencia.

30. Estos sistemas complejos a menudo se caracterizan por ciclos prolongados de diseño y desarrollo, con contratos que pueden haberse firmado antes de que el Reglamento de Ciberresiliencia sea aplicable, por largos períodos de funcionamiento y por un elevado grado de complejidad técnica y organizativa. Dichos sistemas, que se introducirán en el mercado después de la fecha de aplicación del Reglamento de Ciberresiliencia, pueden basarse en componentes introducidos en el mercado antes de que el Reglamento sea aplicable, en arquitecturas consolidadas o en normas de interoperabilidad ampliamente utilizadas, incluidas las normas a las que se hace referencia en otros actos legislativos de la UE o marcos sectoriales específicos. Como consecuencia de ello, es posible que modificar determinadas características técnicas de dichos sistemas, sin afectar a su finalidad prevista, seguridad, fiabilidad o interoperabilidad con la infraestructura existente, sea difícil o requiera un esfuerzo desproporcionado.

31. Estas características no excluyen por sí solas los sistemas complejos del ámbito de aplicación del Reglamento de Ciberresiliencia. Más bien, ilustran la aplicación del enfoque basado en el riesgo del Reglamento, que permite demostrar el cumplimiento de diferentes maneras en función de las características y limitaciones del producto con elementos digitales, de conformidad con su artículo 13, apartado 3. Estas características forman parte de su finalidad prevista y del contexto operativo y, por tanto, son pertinentes a la hora de evaluar el cumplimiento de los requisitos esenciales de ciberseguridad (los «requisitos esenciales»). En particular, el considerando 55 reconoce expresamente que determinados requisitos esenciales pueden no ser plenamente compatibles con la naturaleza de un producto con elementos digitales. Por ejemplo, este puede ser el caso cuando el cumplimiento socave requisitos obligatorios de interoperabilidad o el correcto funcionamiento del sistema.

32. En consecuencia, los fabricantes están obligados a abordar los riesgos de ciberseguridad sobre la base de la evaluación de los riesgos de ciberseguridad a que se refiere el artículo 13, apartado 2. Como también se explica en el considerando 55, en algunos casos, determinados requisitos esenciales no son aplicables o no pueden cumplirse

mediante la aplicación de medidas de seguridad de última generación debido, por ejemplo, a la finalidad prevista del sistema, que exige que el producto con elementos digitales interactúe con dependencias existentes o cumpla determinados requisitos de interoperabilidad. En estos casos, los fabricantes deben identificar y documentar dichas limitaciones específicas, evaluar los riesgos asociados y aplicar medidas alternativas o compensatorias adecuadas de reducción del riesgo, a fin de no socavar la seguridad del producto con elementos digitales. A estos efectos, tanto la documentación técnica a que se refiere el artículo 31 como la información y las instrucciones para el usuario a que se refiere el anexo II desempeñan un papel fundamental a la hora de describir de manera transparente las limitaciones detectadas, los riesgos de ciberseguridad asociados y las medidas de reducción del riesgo aplicadas. De conformidad con la obligación de mantener actualizada la evaluación de riesgos durante el período de soporte, los fabricantes también deben volver a evaluar periódicamente si siguen existiendo tales limitaciones. Cuando dichas limitaciones puedan eliminarse o reducirse con el tiempo, los fabricantes deben actualizar el producto con elementos digitales en consecuencia, de modo que este pueda adquirir un nivel adecuado de ciberseguridad ([10]).

Ejemplo10: un fabricante introduce en el mercado un producto con elementos digitales que se comunica con sistemas externos mediante un protocolo de red. Como parte de la aplicación de los requisitos esenciales, el fabricante determina, sobre la base de la evaluación de los riesgos de ciberseguridad, que es necesario el uso de un protocolo de comunicación seguro para garantizar la confidencialidad e integridad de los datos intercambiados por el producto con elementos digitales.

Sin embargo, su finalidad prevista incluye la interoperabilidad con sistemas existentes que solo admiten un protocolo más antiguo o menos seguro. En tales casos, el fabricante podrá aplicar dicho protocolo cuando sea necesario para lograr la interoperabilidad, siempre que los riesgos de ciberseguridad asociados se detecten y mitiguen por otros medios.

Cuando sea técnicamente viable que el producto con elementos digitales admita tanto el protocolo seguro como el protocolo menos seguro, se espera que el fabricante aplique el protocolo seguro y habilite su uso de forma predeterminada. El protocolo menos seguro solo estaría permitido cuando fuera necesario para garantizar la interoperabilidad.

Ejemplo11: el fabricante de un sistema de automatización industrial adquiere algunos microcontroladores antes de que el Reglamento de Ciberresiliencia sea aplicable. El fabricante lleva a cabo la evaluación de los riesgos de ciberseguridad para su sistema de automatización industrial que se introducirá en el mercado tras la fecha de aplicación del Reglamento. Sobre la base de dicha evaluación de los riesgos de ciberseguridad, el fabricante no detecta riesgos de ciberseguridad específicos asociados al uso de uno de esos microcontroladores. El fabricante lo integra en su sistema de automatización industrial y garantiza que el producto con elementos digitales en su conjunto (el sistema de automatización industrial) cumple los requisitos esenciales.

2.7. **Productos con elementos digitales diseñados antes de la fecha de aplicación del Reglamento de Ciberresiliencia**

33. En algunos casos, un fabricante introducirá en el mercado, tras la fecha de aplicación del Reglamento de Ciberresiliencia el 11 de diciembre de 2027, unidades de un producto con elementos digitales fabricadas de conformidad con un tipo o modelo diseñado y desarrollado antes de la fecha de aplicación del Reglamento. En tales casos, el cumplimiento del Reglamento no exige necesariamente que dichas unidades del producto con elementos digitales se rediseñen. El fabricante debe llevar a cabo una evaluación de los riesgos de ciberseguridad de conformidad con el artículo 13, apartado 2, del Reglamento de Ciberresiliencia para determinar, sobre la base de la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales, cuáles de los requisitos esenciales establecidos en la parte I del anexo I son aplicables a dicho producto con elementos digitales, y cómo se aplican dichos requisitos.

34. Cuando el resultado de la evaluación de los riesgos de ciberseguridad demuestre que el producto con elementos digitales ya incorpora medidas de seguridad adecuadas y eficaces para hacer frente a los riesgos pertinentes, el fabricante podrá basarse en dichas medidas existentes para demostrar el cumplimiento del Reglamento. El Reglamento de Ciberresiliencia no impone por sí mismo la obligación de introducir nuevas características de seguridad ni de rediseñar el producto con elementos digitales cuando ello no sea necesario para hacer frente a los riesgos detectados.

([10]) Cabe señalar que las consideraciones establecidas en este apartado pueden ser aplicables, según proceda, a todos los productos con elementos digitales incluidos en el ámbito de aplicación del Reglamento de Ciberresiliencia, y no únicamente a los «sistemas complejos».

35. No obstante, el fabricante sigue estando sujeto a las obligaciones establecidas en el Reglamento. Estas incluyen asegurarse, antes de que el producto con elementos digitales se introduzca en el mercado, de que se ha llevado a cabo el procedimiento de evaluación de la conformidad aplicable, que se ha elaborado la declaración UE de conformidad y se ha colocado el marcado CE. El cumplimiento de estos requisitos es independiente de que el diseño del producto con elementos digitales haya tenido que modificarse como consecuencia de la evaluación de riesgos. En el caso de los productos con elementos digitales diseñados antes de la fecha de aplicación del Reglamento de Ciberresiliencia, pero introducidos en el mercado después de esa fecha, cuando el fabricante no pueda demostrar cómo se ha tenido en cuenta la evaluación de riesgos durante la fase de diseño y desarrollo del producto con elementos digitales, la obligación establecida en el artículo 13, apartado 2, debe entenderse en el sentido de que exige a los fabricantes llevar a cabo una evaluación de los riesgos de ciberseguridad y demostrar, sobre esa base, que el producto con elementos digitales incorpora medidas de seguridad adecuadas con vistas a minimizar los riesgos de ciberseguridad, prevenir incidentes y minimizar sus efectos, en particular en lo que respecta a la salud y la seguridad de los usuarios.

36. Por consiguiente, los productos con elementos digitales diseñados antes de la fecha de aplicación del Reglamento de Ciberresiliencia podrían introducirse en el mercado de conformidad con dicho Reglamento sin necesidad de rediseñarlos, siempre que el fabricante pueda demostrar, mediante la evaluación de los riesgos de ciberseguridad y la documentación técnica, que el producto con elementos digitales alcanza un nivel adecuado de ciberseguridad a la luz de su finalidad prevista y su uso razonablemente previsible y cumple los requisitos esenciales de ciberseguridad.

37. Además, conviene aclarar la aplicación de las obligaciones de evaluación de la conformidad para los fabricantes de productos con elementos digitales que se introduzcan en el mercado después de la fecha de aplicación del Reglamento de Ciberresiliencia, pero que se hayan fabricado de conformidad con un tipo o modelo diseñado y desarrollado antes de esa fecha. De conformidad con el artículo 13, apartado 12, el fabricante debe demostrar, mediante el procedimiento de evaluación de la conformidad pertinente, que su producto con elementos digitales es conforme con los requisitos esenciales aplicables e incluir pruebas que lo acrediten en la documentación técnica del producto (punto 6 del anexo VII).

38. No obstante, la aplicación de dichos requisitos debe interpretarse a la luz de la evaluación de los riesgos de ciberseguridad y del perfil de riesgo de ciberseguridad del producto con elementos digitales. En particular, en el caso de los productos con elementos digitales diseñados antes de la fecha de aplicación del Reglamento de Ciberresiliencia (pero introducidos en el mercado después de esa fecha) y sujetos a los procedimientos de evaluación de la conformidad establecidos en el artículo 32, apartado 1, cuando la evaluación de riesgos demuestre que el producto con elementos digitales ya incorpora medidas de seguridad adecuadas y eficaces que abordan los riesgos de dicho producto, la obligación de aportar pruebas como parte del procedimiento de evaluación de la conformidad no debe entenderse en el sentido de que exige al fabricante aportar los resultados de las pruebas correspondientes a las fases originales de diseño y desarrollo de dichos productos con elementos digitales. Esto no sería necesario, ya que no contribuiría a aumentar la seguridad del propio producto con elementos digitales. No obstante, cuando puedan ser necesarias pruebas, no se espera que los fabricantes aporten documentación de las pruebas realizadas en todas las variantes de productos, sino que pueden agrupar dichas pruebas en familias de productos con elementos digitales, como se explica con más detalle en la sección *7.4* Reutilización de las evaluaciones de riesgos y la documentación de conformidad para familias de productos con elementos digitales.

39. No obstante, el fabricante debe aportar pruebas de cómo cumple los procesos de gestión de las vulnerabilidades establecidos en la parte II del anexo I, así como mantener actualizada su evaluación de riesgos de conformidad con el artículo 13, apartado 3, y cumplir todas las demás obligaciones establecidas en el Reglamento de Ciberresiliencia, en particular la de proporcionar a los usuarios información e instrucciones de conformidad con el artículo 13, apartado 18.

Ejemplo12: un fabricante introduce en el mercado un microcontrolador diseñado y desarrollado antes de la fecha de aplicación del Reglamento de Ciberresiliencia. El microcontrolador está destinado a integrarse en una serie de productos electrónicos con elementos digitales, entre ellos productos con elementos digitales con funcionalidades de conectividad.

Antes de introducir en el mercado nuevas unidades del microcontrolador una vez que el Reglamento de Ciberresiliencia sea aplicable, el fabricante lleva a cabo una evaluación de los riesgos de ciberseguridad de conformidad con el artículo 13, apartado 2. Sobre la base de la finalidad prevista del microcontrolador y de su uso razonablemente previsible, el fabricante determina los riesgos de ciberseguridad pertinentes, como el acceso no autorizado, la manipulación de programas informáticos o datos y el uso indebido de las interfaces disponibles.

El resultado de la evaluación de riesgos pone de manifiesto que el microcontrolador, tal como se diseñó originalmente, ya incorpora medidas de seguridad adecuadas y eficaces para hacer frente a los riesgos detectados. Así pues, el fabricante concluye que el producto con elementos digitales cumple los requisitos esenciales pertinentes establecidos en la parte I del anexo I, y que no es necesario rediseñarlo ni introducir funcionalidades de seguridad adicionales.

En los casos en que no es posible demostrar cómo se tuvo en cuenta una evaluación de los riesgos de ciberseguridad durante la fase original de diseño y desarrollo, el fabricante documenta una evaluación de los riesgos de ciberseguridad actual y explica cómo el diseño y las medidas existentes mitigan los riesgos detectados. El fabricante no está obligado a recrear la documentación de diseño o de las pruebas realizadas correspondiente a fases anteriores, ya que esto no contribuiría a mejorar la ciberseguridad del producto con elementos digitales. Cuando distintas variantes del microcontrolador se basen en el mismo diseño y compartan el mismo perfil de riesgo de ciberseguridad, el fabricante también podrá basarse en pruebas representativas que abarquen la familia de productos pertinente.

El fabricante también garantiza el cumplimiento de los requisitos de gestión de las vulnerabilidades establecidos en la parte II del anexo I, entre otras cosas, manteniendo procesos para abordar y subsanar las vulnerabilidades y revisando la evaluación de los riesgos de ciberseguridad de conformidad con el artículo 13, apartado 3, del Reglamento.

En estas circunstancias, el microcontrolador diseñado antes de la fecha de aplicación del Reglamento de Ciberresiliencia podrá introducirse en el mercado sin necesidad de rediseñarlo, siempre que el fabricante pueda demostrar, mediante la evaluación de los riesgos de ciberseguridad y la documentación técnica, que el microcontrolador alcanza un nivel adecuado de ciberseguridad a la luz de su finalidad prevista y su uso razonablemente previsible y cumple los requisitos esenciales aplicable.

3. **PROGRAMAS INFORMÁTICOS LIBRES Y DE CÓDIGO ABIERTO**

40. Como se recuerda en la sección *2.1* Introducción en el mercado, el Reglamento de Ciberresiliencia se aplica a los productos con elementos digitales comercializados por primera vez en el mercado de la UE en el transcurso de una actividad comercial (es decir, «introducidos en el mercado»), así como a cualquier caso posterior que constituya comercialización de ese mismo producto con elementos digitales. La Guía azul (sección 2.2) aclara que por «actividad comercial» debe entenderse el suministro de mercancías, ya sea a título oneroso o gratuito, en un contexto empresarial y solo puede determinarse caso por caso, teniendo en cuenta la regularidad de los suministros, las características del producto, las intenciones del proveedor, etc.

41. El suministro en el transcurso de una actividad comercial se caracteriza por una serie de circunstancias, que se documentan de forma extensa en la Guía azul y se recuerdan en el considerando 15 del Reglamento de Ciberresiliencia. Estas pueden incluir la aplicación directa de un precio, así como también «la aplicación de un precio a los servicios de asistencia técnica, cuando esta no se utilice únicamente para la recuperación de costes efectivos, mediante la intención de monetizar, por ejemplo por el suministro de una plataforma de software a través de la cual el fabricante monetiza otros servicios, requiriendo como condición para el uso el tratamiento de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático, o la aceptación de donaciones que excedan los costes asociados con el diseño, desarrollo y suministro de un producto con elementos digitales» (considerando 15 del Reglamento de Ciberresiliencia) ([11]).

42. Sin embargo, el Reglamento de Ciberresiliencia reconoce las especificidades de las diferentes formas de desarrollar y publicar «programas informáticos libres y de código abierto» y ofrece algunas orientaciones para ayudar a determinar si un programa de este tipo es un producto con elementos digitales introducido en el mercado (esto es, en el transcurso de una actividad comercial) en el sentido del Reglamento de Ciberresiliencia. Como se explica en el considerando 18, «las circunstancias en las que el producto con elementos digitales se ha desarrollado o el modo en que se ha financiado el desarrollo no se han de tener en cuenta a la hora de determinar el carácter comercial o no comercial de dicha actividad». Más concretamente, «a fin de garantizar que exista una distinción clara entre las fases de desarrollo y suministro, el suministro de productos con elementos digitales que se consideren programas informáticos libres y de código abierto que no sean monetizados por sus fabricantes no debe considerarse una actividad comercial».

([11]) También cabe recordar que, si bien los productos con elementos digitales a menudo se monetizan (también) mediante el tratamiento de datos personales, la protección de los datos personales es un derecho fundamental y, por lo tanto, los datos personales no pueden considerarse una mercancía, como se indica en el considerando 24 de la Directiva 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (DO L 136 de 22.5.2019, p. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Por lo tanto, conviene i) aclarar qué es un programa informático libre y de código abierto; ii) cuando se considera que está bajo la responsabilidad de una persona física o jurídica; y iii) proporcionar ejemplos para ayudar a las partes interesadas a comprender cuándo la distribución de un programa informático libre y de código abierto constituye una introducción en el mercado. Cuando el programa informático libre y de código abierto no se introduce en el mercado, queda fuera del ámbito de aplicación del Reglamento de Ciberresiliencia, salvo que la entidad que lo publica sea una persona jurídica que se ajuste a la definición de «administrador de comunidad de programas informáticos de código abierto» (en lo sucesivo, «administrador») con arreglo al artículo 3, punto 14. En este caso, solo estará sujeto a las obligaciones establecidas en el artículo 24.

44. El artículo 3, punto 48, define un «programa informático libre y de código abierto» como un «programa informático cuyo código fuente se comparte abiertamente y que se ofrece con arreglo a una licencia libre y de código abierto que abarca todos los derechos para que el programa informático sea libremente accesible, utilizable, modificable y redistribuible». Aunque las presentes orientaciones no determinan las licencias específicas de programas informáticos libres y de código abierto que son compatibles con la definición establecida en el artículo 3, punto 48, de la redacción de dicha disposición se desprende que, a efectos del Reglamento de Ciberresiliencia, solo se consideran programas informáticos libres y de código abierto los programas informáticos que cumplan acumulativamente dos condiciones: i) el programa informático debe ponerse a disposición con arreglo a una licencia libre y de código abierto que conceda el conjunto completo de derechos a que se refiere el artículo 3, punto 48; y ii) su código fuente debe compartirse abiertamente.

45. El requisito de que la licencia establezca que el programa informático sea «libremente accesible, utilizable, modificable y redistribuible» refleja la interpretación tradicional que se hace del programa informático libre y de código abierto, según la cual los usuarios deben poder acceder al código fuente, utilizarlo sin restricciones indebidas, modificarlo y redistribuir versiones originales o modificadas. Por lo tanto, el acceso al código fuente es una condición previa necesaria para el ejercicio de los demás derechos: sin acceso al código fuente, no es posible en la práctica modificar el programa informático ni reutilizarlo de manera significativa.

46. No obstante, el artículo 3, punto 48, no se limita a establecer las condiciones de la licencia, ya que exige expresamente que el código fuente «se comparta abiertamente». Esto significa que el código fuente debe ponerse a disposición del público (tanto *upstream* como *downstream*), y no proporcionarse únicamente de forma restringida o condicionada. Por consiguiente, los programas informáticos distribuidos con arreglo a una licencia de código abierto, pero cuyo código fuente solo se comparte (o está permitido compartirlo) con clientes de pago o un grupo limitado de usuarios, no deben considerarse programas informáticos libres y de código abierto en el sentido del artículo 3, punto 48. Por tanto, a efectos del Reglamento de Ciberresiliencia, solo deben considerarse programas informáticos libres y de código abierto los programas informáticos cuyo código fuente esté disponible públicamente y que se distribuyan con arreglo a una licencia de código abierto que conceda el conjunto completo de derechos a que se refiere el artículo 3, punto 48.

3.1. **Determinación de cuándo un programa informático libre y de código abierto se considera responsabilidad de una persona**

47. El Reglamento de Ciberresiliencia impone responsabilidades clave a los operadores económicos que suministran productos con elementos digitales en el mercado de la UE. Define al fabricante como la persona física o jurídica que suministra un producto con elementos digitales con su nombre o marca comercial y que lo hace en el transcurso de una actividad comercial (introduciéndolo de este modo en el mercado). Del mismo modo, un importador es la persona física o jurídica establecida en la UE que suministra el producto con elementos digitales de una persona establecida fuera de la UE, y que lo hace en el transcurso de una actividad comercial (introduciéndolo de este modo en el mercado). Las obligaciones de los administradores se aplican a la persona jurídica que suministra un programa informático libre y de código abierto destinado a actividades comerciales ([12]), pero no lo introduce en el mercado en el sentido del Reglamento de Ciberresiliencia.

48. Por lo tanto, para determinar si una persona física o jurídica está introduciendo un programa informático libre y de código abierto en el mercado de la UE, en primer lugar debe aclararse si dicha persona física o jurídica está efectivamente suministrando el programa informático libre y de código abierto. Para establecer correctamente las obligaciones aplicables en virtud del Reglamento de Ciberresiliencia, es fundamental determinar si la persona física o jurídica está efectivamente llevando a cabo la acción de suministrar el programa informático libre y de código abierto. De hecho, como se recuerda en el considerando 18, el Reglamento de Ciberresiliencia no se aplica a las personas físicas o jurídicas que contribuyen con código fuente a productos con elementos digitales que cumplen los requisitos para considerarse programas informáticos libres y de código abierto y que no están bajo su responsabilidad.

([12]) Se trata de una condición necesaria, aunque no suficiente, para que una persona jurídica pueda considerarse administrador de comunidad de programas informáticos de código abierto, ya que la definición recogida en el artículo 3, punto 14, establece condiciones adicionales para que una persona jurídica pueda considerarse administrador.

49. Habida cuenta de las particularidades del desarrollo de los programas informáticos libres y de código abierto, que a menudo implica a múltiples colaboradores, modelos de colaboración descentralizada y una separación entre la contribución y la toma de decisiones, conviene aclarar que se considera que el programa informático libre y de código abierto «está bajo la responsabilidad» de las personas físicas o jurídicas que lo publican y ejercen el control principal sobre su desarrollo, versiones y decisiones de distribución (a menudo denominados «encargados del mantenimiento»). Las personas que contribuyen con código fuente pero no controlan las versiones, las hojas de ruta ni las decisiones en materia de gobernanza se consideran «colaboradores»; en tales casos, el programa informático libre y de código abierto no está bajo su responsabilidad, aunque hayan contribuido con código al mismo. La mera existencia de permisos técnicos, como el acceso para realizar cambios (*commit*), no basta para determinar que el programa informático libre y de código abierto está bajo la responsabilidad de dicha persona; la responsabilidad recae en quienes lo publican y lo controlan.

*Ejemplo 13: un desarrollador independiente o un empleado de una empresa presenta una solicitud de incorporación de cambios (*pull request *o* merge request*) que contiene un parche de seguridad o una nueva funcionalidad para el proyecto de un programa informático libre y de código abierto. Los encargados del mantenimiento del proyecto revisan, aceptan e incorporan el código en el repositorio principal, y lo incluyen posteriormente en una nueva versión. En este escenario, la persona que presentó la solicitud de incorporación de cambios es un «colaborador» y no está sujeta al Reglamento de Ciberresiliencia. Aunque esa persona contribuyó con código fuente, no ejerce el control principal sobre las decisiones relativas al desarrollo, las versiones o la distribución.*

3.2. **Determinación de cuándo un programa informático libre y de código abierto se introduce en el mercado de la UE**

50. Una vez que se determina que un programa informático libre y de código abierto es responsabilidad de una persona física o jurídica, debe establecerse si dicha persona lo suministra en el transcurso de una actividad comercial, lo que constituye una introducción en el mercado.

3.2.1. *Cobro de un precio*

51. Cuando la persona física o jurídica que suministra un programa informático libre y de código abierto cobra un precio por el propio programa informático (por ejemplo, cobrando un precio por los binarios precompilados), dicha persona está introduciendo un producto con elementos digitales en el mercado. Por lo tanto, la persona que introduce un programa informático libre y de código abierto en el mercado se considera un fabricante a efectos del Reglamento de Ciberresiliencia.

52. A menudo, los fabricantes de programas informáticos libres y de código abierto suministran gratuitamente versiones de dicho programa informático (suelen denominarse versiones «comunitarias»), cuya base de código es (prácticamente) idéntica a la de la versión de pago. Sin embargo, estos productos con elementos digitales son diferentes: la versión de pago se monetiza de alguna manera (por ejemplo, mediante el cobro de un precio o por otros medios, como se analiza en la presente sección), por lo que se considera introducida en el mercado, lo que da lugar a que se apliquen las obligaciones del fabricante. La versión facilitada de forma gratuita (o versión comunitaria) no se monetiza, por lo que no se considera introducida en el mercado a efectos del Reglamento de Ciberresiliencia. Este es también el caso cuando la versión de pago es una versión comercial «mejorada» que amplía la base de código de la versión facilitada gratuitamente, o incorpora dicha versión a un producto con elementos digitales más amplio (por ejemplo, como ocurre en el modelo de «núcleo abierto»).

53. Si la persona que suministra la versión comunitaria es una persona jurídica, dicha persona jurídica también está sujeta a las obligaciones aplicables a los administradores en relación con la versión que suministra gratuitamente (la versión comunitaria). Si la entidad es una persona física, la versión proporcionada gratuitamente (la versión comunitaria) no entra en el ámbito de aplicación del Reglamento de Ciberresiliencia.

3.2.2. *Monetización de otros servicios o exigencia del tratamiento de datos personales*

54. Una persona física o jurídica que publique un programa informático libre y de código abierto también puede estar introduciéndolo en el mercado (es decir, suministrándolo en el transcurso de una actividad comercial) cuando proporcione el programa informático a través del cual monetiza otros productos con elementos o servicios digitales, o cuando exija, como condición para su uso, el tratamiento de datos personales por motivos distintos de la mejora exclusiva de la seguridad, la compatibilidad o la interoperabilidad del programa informático.

Ejemplo 14: una persona física o jurídica publica una aplicación de mercado libre y de código abierto. La aplicación está disponible de forma gratuita y permite a los usuarios adquirir bienes o servicios a través de ella. La aplicación permite a la persona que la publicó monetizar otros productos con elementos digitales y servicios ofrecidos a través de ella (por ejemplo, mediante anuncios, comisiones de intermediario o cuotas de suscripción). Por lo tanto, se considera que la aplicación se ha introducido en el mercado en el transcurso de una actividad comercial.

Ejemplo15: una persona física o jurídica publica una VPN libre y de código abierto. La aplicación está disponible de forma gratuita, pero permite a los usuarios pagar para acceder a servidores adicionales o direcciones IP específicas. Esta aplicación permite a dicha persona monetizar otros servicios que se ofrecen a través de ella, por lo que se considera introducida en el mercado en el transcurso de una actividad comercial.

Ejemplo16: una persona física o jurídica publica una aplicación para el seguimiento de la actividad física libre y de código abierto. La aplicación está disponible de forma gratuita, pero su uso está condicionado al tratamiento de los datos personales de los usuarios con fines como la publicidad personalizada o el análisis que no guardan relación con la seguridad, la compatibilidad o la interoperabilidad del programa informático. Al exigir dicho tratamiento de datos como condición para su uso, se considera, por tanto, que la aplicación se ha introducido en el mercado en el transcurso de una actividad comercial.

3.2.3. *Servicios de asistencia*

55. El mero hecho de que una persona física o jurídica que publica un programa informático libre y de código abierto también ofrezca servicios de asistencia de pago relacionados con dicho programa no significa, por sí solo, que el producto con elementos digitales se suministre en el transcurso de una actividad comercial. Los servicios de asistencia pueden incluir actividades como servicios de consultoría y de formación o servicios profesionales relacionados con el uso, la documentación, la configuración y la implantación del programa informático por parte de un cliente.

56. El factor decisivo es si el acceso al propio programa informático libre y de código abierto (es decir, el suministro del producto con elementos digitales), incluido su mantenimiento, está supeditado a una remuneración, y no el mero hecho de ofrecer servicios profesionales relacionados con un producto con elementos digitales disponible gratuitamente, como se indica en el considerando 18 del Reglamento de Ciberresiliencia («el suministro de productos con elementos digitales que se consideren programas informáticos libres y de código abierto que no sean monetizados por sus fabricantes no debe considerarse una actividad comercial»). Si el programa informático libre y de código abierto puede descargarse e instalarse de forma gratuita y los usuarios pueden optar por adquirir servicios profesionales por separado, no se considera que dicho programa se haya introducido en el mercado.

57. En cambio, en algunos casos, el acceso a una versión específica del producto con elementos digitales que incluya determinadas prestaciones, como la asistencia técnica o la optimización del rendimiento, está supeditado a una remuneración. En tales casos, dicho suministro constituye un suministro monetizado de un producto con elementos digitales realizado en el transcurso de una actividad comercial y, por tanto, se considera que el producto se ha introducido en el mercado. Esto incluye los casos en que una edición de pago o una versión empresarial se pone a disposición en virtud de un acuerdo comercial, independientemente de que también esté disponible de forma gratuita un programa informático funcionalmente equivalente con arreglo a una licencia de programas informáticos libres y de código abierto.

Ejemplo17: una persona física o jurídica publica un sistema operativo gratuito y de código abierto, y ofrece una versión de pago de dicho sistema operativo que incluye servicios de asistencia, como soporte técnico u optimización del rendimiento. Se considera que la versión de pago del sistema operativo se ha introducido en el mercado en el transcurso de una actividad comercial.

Ejemplo18: una persona física o jurídica publica una herramienta de línea de comandos libre y de código abierto. La herramienta está disponible de forma gratuita y cualquier persona puede descargarla e instalarla. Dicha persona física o jurídica ofrece por separado servicios profesionales, como servicios de consultoría opcionales para formar a los usuarios y ayudarles a instalar y utilizar la herramienta. No se considera que dicho programa informático libre y de código abierto se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia.

58. En particular, en el caso de las personas físicas que publican programas informáticos libres y de código abierto, ofrecer asistencia técnica directamente vinculada al acceso al producto con elementos digitales seguiría sin considerarse una actividad comercial si, como se indica en el considerando 15 del Reglamento de Ciberresiliencia, la aplicación de un precio solo sirve para la recuperación de costes efectivos. Estos costes efectivos incluyen una variedad de costes relacionados con el diseño, el desarrollo y el mantenimiento del programa informático, incluidos los gastos razonables de subsistencia de la persona. Por lo tanto, no debe considerarse que una persona física que publique un programa informático libre y de código abierto y ofrezca asistencia técnica para cubrir sus costes y obtener una remuneración justa esté introduciendo, por ese mero hecho, dicho programa informático en el mercado de la UE.

59. No se considerará que una persona física o jurídica que ofrezca asistencia técnica relacionada con un programa informático libre y de código abierto que esté bajo su responsabilidad esté introduciendo dicho programa informático en el mercado, salvo que la persona en cuestión modifique sustancialmente el programa informático libre y de código abierto, de conformidad con el artículo 22, como parte de la prestación de dicha asistencia.

Ejemplo19: un prestador de servicios no publica un programa informático libre y de código abierto, sino que ayuda a un cliente a instalarlo en el servidor local del cliente. Lo hace sin llevar a cabo una modificación sustancial del programa informático libre y de código abierto. Por lo tanto, no se considera que el prestador de servicios esté introduciendo dicho programa informático libre y de código abierto en el mercado.

3.2.4. *Donaciones*

60. Las personas físicas o jurídicas que publican proyectos de programas informáticos libres y de código abierto suelen incluir medios para que los usuarios de dicho programa informático puedan donar dinero de forma voluntaria a modo de agradecimiento a quienes los publican y también para garantizar el mantenimiento activo del proyecto.

61. Como se indica en el considerando 15 del Reglamento de Ciberresiliencia, «[l]a aceptación de donaciones sin la intención de obtener un beneficio no debe considerarse una actividad comercial». El mero hecho de incluir un enlace a una plataforma de donaciones o herramientas similares para recaudar donaciones no debe considerarse una intención de obtener beneficios, aun cuando el importe recaudado a través de las donaciones supere los costes asociados al diseño, el desarrollo y el suministro de un producto con elementos digitales. Esto incluye una compensación razonable para los colaboradores contratados por una persona jurídica o los gastos razonables de subsistencia de una persona física. Las donaciones, por su propia naturaleza, fluctúan a lo largo del tiempo, por lo que debe aplicarse cierto grado de flexibilidad a la hora de evaluar si se considera que un programa informático libre y de código abierto monetizado exclusivamente mediante donaciones se ha introducido en el mercado. Por lo tanto, es poco probable que un programa informático libre y de código abierto financiado exclusivamente mediante donaciones se considere introducido en el mercado en el sentido del Reglamento de Ciberresiliencia.

Ejemplo 20: una persona física o jurídica publica una herramienta de programa informático libre y de código abierto en un repositorio público en línea, lo que permite a cualquier persona descargarla, utilizarla, modificarla y redistribuirla con arreglo a una licencia de programas informáticos libres y de código abierto. La persona que la publica invita a los usuarios a realizar donaciones voluntarias a través de una plataforma de donaciones para apoyar el desarrollo y el mantenimiento continuos del proyecto. El acceso al programa informático, a su código fuente y a sus actualizaciones no depende de que se realice una donación. No se considera que dicho programa informático libre y de código abierto se suministre en el transcurso de una actividad comercial ni que se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia.

62. No obstante, hay casos en los que puede considerarse que un programa informático libre y de código abierto financiado mediante donaciones se ha introducido en el mercado. Este es el caso cuando, sobre la base de una evaluación global de las circunstancias, las donaciones son, de hecho, equivalentes al cobro de un precio para acceder al producto con elementos digitales o a algunas de sus funcionalidades. Esto puede ocurrir, en particular, cuando el acceso al programa informático libre y de código abierto, a las funcionalidades esenciales o a las actualizaciones está condicionado en la práctica a que se realice una donación, o cuando las donaciones están asociadas a beneficios contractuales o ventajas exclusivas que van más allá de las ventajas propias de la comunidad.

Ejemplo 21: una persona física o jurídica publica un producto con elementos digitales consistente en un programa informático con arreglo a una licencia de programas informáticos libres y de código abierto, pero proporciona versiones descargables y actualizaciones de seguridad solo a los usuarios que realizan una donación. Los usuarios que no realizan una donación no tienen acceso a la versión actual del programa informático.

En este caso, las donaciones constituyen, de hecho, una condición para acceder al producto con elementos digitales y, por lo tanto, equivalen al cobro de un precio. Por lo tanto, se considera que dicho programa informático libre y de código abierto se ha introducido en el mercado en el sentido del Reglamento de Ciberresiliencia.

Ejemplo 22: una persona física o jurídica pone a disposición del público el código fuente de un programa informático libre y de código abierto, pero proporciona los binarios precompilados, las actualizaciones periódicas y las correcciones de seguridad garantizadas solo a las personas que realizan una donación. En este caso, las donaciones están vinculadas al acceso a aspectos esenciales del producto con elementos digitales y constituyen una remuneración por el suministro de dicho producto. Por lo tanto, se considera que dicho programa informático libre y de código abierto se ha introducido en el mercado en el transcurso de una actividad comercial.

3.2.5. *Financiación de programas informáticos libres y de código abierto*

63. El mero hecho de que un tercero haya pagado, patrocinado o financiado de otro modo el desarrollo de un programa informático libre y de código abierto no determina por sí solo si dicho programa informático se ha introducido en el mercado o no. Es práctica común en el ecosistema de los programas informáticos libres y de código abierto que desarrolladores independientes, fundaciones o comunidades reciban financiación de empresas, organismos públicos u otros patrocinadores con el fin de trabajar en funcionalidades específicas, corregir errores o mantener componentes esenciales. Esta financiación puede adoptar diversas formas, como subvenciones, recompensas por la detección de errores, patrocinios, contratos de servicios o trabajos de desarrollo remunerados.

64. Como ya se ha señalado, el considerando 18 del Reglamento de Ciberresiliencia aclara que las circunstancias en las que el producto con elementos digitales se ha desarrollado o el modo en que se ha financiado el desarrollo no se han de tener en cuenta a la hora de determinar el carácter comercial de dicha actividad.

65. Por lo tanto, cuando el programa informático libre y de código abierto se comparte abiertamente y se pone a disposición de todos de forma gratuita para que puedan acceder a él, utilizarlo, modificarlo y redistribuirlo, el hecho de que una entidad comercial pueda haber pagado por dicho proyecto no debe tenerse en cuenta para determinar si el programa informático se ha introducido en el mercado. De hecho, si dicho programa informático libre y de código abierto no se monetiza de otro modo, no debe considerarse introducido en el mercado. Cuando la empresa que financió el desarrollo del programa informático libre y de código abierto (así como cualquier otra empresa) lo integre en su producto con elementos digitales, dicha empresa debe ejercer la diligencia debida de conformidad con el artículo 13, apartado 5, del Reglamento de Ciberresiliencia.

Ejemplo 23: un desarrollador independiente publica un proyecto de programa informático libre y de código abierto y lo mantiene de forma activa. El fabricante A solicita que el desarrollador independiente añada una funcionalidad específica al programa informático libre y de código abierto, y financia dicho desarrollo. El desarrollador añade la funcionalidad a la base de código del programa informático libre y de código abierto, compartiéndolo abiertamente y poniéndolo a disposición de todos de forma gratuita para que puedan acceder a él, utilizarlo, modificarlo y redistribuirlo. No se considera que el desarrollador independiente haya introducido dicho programa informático libre y de código abierto en el mercado. Si el fabricante integra el programa informático libre y de código abierto en su producto con elementos digitales, debe ejercer la diligencia debida de conformidad con el artículo 13, apartado 5, del Reglamento de Ciberresiliencia.

3.2.6. *Entidades sin ánimo de lucro constituidas para alcanzar objetivos sin ánimo de lucro*

66. Cuando una persona jurídica que publica un programa informático libre y de código abierto es una organización sin ánimo de lucro que «se haya establecido de tal manera que se garantice que todos los ingresos después de los costes se utilicen para alcanzar objetivos sin ánimo de lucro» (considerando 18 del Reglamento de Ciberresiliencia), no se considera que el programa informático libre y de código abierto que publica se haya introducido en el mercado. Cuando dicha persona jurídica se ajusta a la definición de «administrador», entonces estará sujeta a las obligaciones correspondientes (artículo 24 del Reglamento de Ciberresiliencia).

Ejemplo 24: una persona jurídica publica un navegador gratuito y de código abierto que se monetiza directamente mediante acuerdos con motores de búsqueda, pero todos sus ingresos después de los costes se utilizan para objetivos sin ánimo de lucro. No se considera que el navegador se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia. La persona jurídica que publica el navegador está sujeta a las obligaciones aplicables a los administradores.

3.2.7. *Integración por parte de otros fabricantes*

67. En algunos casos, una persona física o jurídica claramente identificable publica un programa informático libre y de código abierto, pero dicho programa informático está destinado a ser integrado por otros fabricantes en sus propios productos con elementos digitales. En tales casos, no se considera que dicho programa informático libre y de código abierto se haya introducido en el mercado de la UE, salvo que la persona que lo publica (es decir, el fabricante original) también lo monetice, en consonancia con las secciones anteriores de las presentes orientaciones.

68. Si el programa informático libre y de código abierto no se introduce en el mercado, la persona jurídica que lo publica estará sujeta a las obligaciones aplicables a los administradores si presta apoyo de forma continuada, de conformidad con la definición de «administrador».

Ejemplo 25: una persona jurídica publica una biblioteca de programas informáticos libres y de código abierto para crear interfaces de usuario. No monetiza el suministro de dicha biblioteca, sino que la integra en uno de sus productos con elementos digitales (que, a su vez, se introduce en el mercado). No se considera que la biblioteca se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia, sino que está destinada a integrarse en productos con elementos digitales. La persona jurídica que la publica es su administrador.

Ejemplo 26: una persona jurídica introduce un sistema operativo en el mercado y también publica bibliotecas de programas informáticos libres y de código abierto que sirven como implementaciones de referencia para los usuarios de dicho sistema operativo. La persona jurídica no monetiza las bibliotecas de programas informáticos libres y de código abierto, que están destinadas a integrarse en otros productos con elementos digitales. La persona jurídica que las publica se considera su administrador.

3.3. **Administradores de comunidad de programas informáticos de código abierto**

69. El Reglamento de Ciberresiliencia introduce la nueva categoría jurídica de «administrador de comunidad de programas informáticos de código abierto» a la luz de «la importancia para la ciberseguridad de muchos productos con elementos digitales que se consideran programas informáticos libres y de código abierto que se publican, pero no se comercializan en el sentido del [Reglamento de Ciberresiliencia]» (considerando 19 del Reglamento).

70. En algunos casos, una persona jurídica que «tiene la finalidad o el objetivo de dar soporte sistemáticamente y de forma sostenida para el desarrollo de [programas informáticos libres y de código abierto] [...] y estén destinados a actividades comerciales, y que garantiza la viabilidad de dichos productos» (artículo 3, punto 14, del Reglamento) publica un programa informático libre y de código abierto pero no lo comercializa en el sentido del Reglamento de Ciberresiliencia. En tales casos, dicha persona jurídica está sujeta a las obligaciones de los administradores.

71. Un administrador se define como una «persona jurídica, distinta de un fabricante», porque el fabricante, por definición, es la persona física o jurídica que introduce en el mercado productos con elementos digitales («los comercializa») con su propio nombre o marca comercial. Una persona jurídica solo puede ser administrador de productos con elementos digitales que reúnan las condiciones para considerarse programas informáticos libres y de código abierto que se publiquen, pero que no se comercialicen en el sentido del Reglamento de Ciberresiliencia. Por lo tanto, el concepto de administrador se aplica a casos concretos de programas informáticos libres y de código abierto que «estén destinados en última instancia a actividades comerciales, como la integración en servicios comerciales o en productos monetizados con elementos digitales» (considerando 19 del Reglamento de Ciberresiliencia ([13])), pero que no se comercialicen en el sentido del Reglamento, y respecto de los cuales la persona jurídica que publica el programa informático libre y de código abierto garantice un soporte sistemático.

72. Ser administrador de un programa informático libre y de código abierto específico no significa que esa persona jurídica sea necesariamente también administrador de otro programa informático libre y de código abierto que publique. Del mismo modo, ser fabricante de un programa informático libre y de código abierto específico no significa que la persona jurídica no pueda ser administrador de otro programa informático libre y de código abierto. Esto incluye proporcionar versiones «comunitarias» del mismo programa informático libre y de código abierto, tal como se describe en la sección *3.2.1* Cobro de un precio.

73. Por lo tanto, una persona jurídica puede ser simultáneamente administrador de un programa informático libre y de código abierto específico (para el que el administrador da soporte sistemáticamente de forma continuada y garantiza la viabilidad del programa informático) y fabricante de otro programa informático libre y de código abierto específico (que introduce en el mercado). En otras palabras, puede exigirse a la misma entidad jurídica que desempeñe distintas funciones para diferentes proyectos de programa informático libre y de código abierto.

74. Para cada programa informático libre y de código abierto específico que publique, la persona jurídica deberá determinar si dicho programa informático se considera introducido en el mercado en el sentido del Reglamento de Ciberresiliencia. En caso afirmativo, esto convierte a la persona jurídica en el fabricante del programa informático. Si no se considera que el programa informático libre y de código abierto se ha introducido en el mercado, la persona jurídica puede ser su administrador si el programa informático está destinado a actividades comerciales y si la persona jurídica lo mantiene de conformidad con la definición de «administrador» ([14]).

3.3.1. *Apoyo continuado y garantía de la viabilidad del programa informático libre y de código abierto*

75. El considerando 19 explica que la prestación de apoyo continuado al desarrollo de un producto con elementos digitales puede incluir (entre otras cosas): i) el alojamiento y la gestión de plataformas de colaboración para el desarrollo de programas informáticos; ii) el alojamiento de códigos fuente o programas informáticos; iii) la administración o gestión de productos con elementos digitales que se consideren programas informáticos libres y de código abierto; y iv) la dirección del desarrollo de dichos productos con elementos digitales.

76. Este puede ser el caso, por ejemplo, de una entidad jurídica que desarrolle un programa informático libre y de código abierto para integrarlo en sus propios productos con elementos digitales y, a continuación, lo publique sin introducirlo en el mercado. Esta cuestión también se analiza en la sección *3.2.7* Integración por parte de otros fabricantes. En este caso, la entidad jurídica no es un fabricante del programa informático, pero puede ser administrador del mismo. Además, como también se ha explicado en secciones anteriores, una entidad jurídica que publique una versión gratuita (o comunitaria) y una versión monetizada del mismo programa informático libre y de código abierto se considera administrador de la versión gratuita (o comunitaria) y fabricante de la versión monetizada.

77. Del mismo modo, una entidad jurídica que monetiza un programa informático libre y de código abierto, pero es una entidad sin ánimo de lucro cuyos ingresos después de los costes se utilizan para alcanzar objetivos sin ánimo de lucro (y, por tanto, su programa informático libre y de código abierto no se introduce en el mercado en el sentido del Reglamento de Ciberresiliencia, tal como se explica en la sección *3.2.6* Entidades sin ánimo de lucro constituidas para alcanzar objetivos sin ánimo de lucro), es administrador del programa informático libre y de código abierto que publica.

78. Además, algunas fundaciones ofrecen plataformas de colaboración con diversas formas de gobernanza que permiten a los fabricantes contribuir de forma habitual al desarrollo de programas informáticos libres y de código abierto o que reciben financiación periódicamente de los fabricantes. Estas fundaciones deben considerarse administradores en relación con programas informáticos libres y de código abierto específicos que estén destinados a actividades comerciales y para los que la fundación preste apoyo continuado. No obstante, como se explica en la sección *3.3* Administradores de comunidad de programas informáticos de código abierto, es posible que una fundación de este tipo no esté sujeta a ninguna obligación en virtud del Reglamento de Ciberresiliencia en relación con otros programas informáticos libres y de código abierto específicos que aloje, en los casos en que no preste soporte sistemático a un programa informático libre y de código abierto específico, no garantice su viabilidad o cuando dicho programa informático específico no esté destinado a actividades comerciales.

([13]) Este concepto también figura en la formulación «destinados en última instancia a actividades comerciales» incluida en la definición de «administrador de comunidad de programas informáticos de código abierto» que figura en el artículo 3, punto 14, del Reglamento de Ciberresiliencia.

([14]) También es posible que la persona jurídica no esté sujeta a ninguna obligación en virtud del Reglamento de Ciberresiliencia, si: i) no se introduce en el mercado un programa informático libre y de código abierto específico en el sentido del Reglamento de Ciberresiliencia; y ii) la entidad jurídica no se ajusta a la definición de «administrador» en relación con dicho programa informático libre y de código abierto específico.

79. El tipo de «apoyo sostenido» que las fundaciones y organizaciones similares prestan a proyectos de programas informáticos libres y de código abierto específicos puede variar considerablemente. Por ejemplo, determinadas entidades jurídicas solo prestan asistencia no técnica, como gestionar la marca de los proyectos, establecer normas de gobernanza, organizar actos de la comunidad o recaudar donaciones. Otras entidades también proporcionan la infraestructura informática subyacente necesaria para ejecutar el proyecto, como alojar repositorios de código fuente, proporcionar sistemas de control de versiones o generar claves de firma. Otras van más allá en el tipo de apoyo que prestan y contribuyen activamente con recursos de ingeniería al proyecto, por ejemplo, contratando desarrolladores, coordinando las labores de desarrollo, revisando o incorporando código, gestionando versiones o encargándose de informes de vulnerabilidades y parches de seguridad. Si bien todas las entidades jurídicas que reúnen las condiciones para ser administradores en virtud del Reglamento de Ciberresiliencia están obligadas a cumplir las obligaciones establecidas en el artículo 24, apartados 1 y 2, el alcance de la aplicación de las obligaciones establecidas en el artículo 14, apartados 1, 3 y 8, a dichas entidades jurídicas varía en función del tipo de apoyo que presten, de conformidad con el artículo 24, apartado 3.

80. Por ejemplo, un administrador que solo presta asistencia no técnica, por definición, no participa en el desarrollo del producto con elementos digitales, por lo que no está obligado a notificar vulnerabilidades aprovechadas activamente. Ese administrador tampoco proporciona redes ni sistemas de información para el desarrollo de dichos productos con elementos digitales, por lo que no está obligado a notificar incidentes graves a la ENISA y a los equipos de respuesta a incidentes de seguridad informática (CSIRT) ni a los usuarios afectados. No obstante, cuando el administrador tenga conocimiento de una vulnerabilidad aprovechada activamente (por ejemplo, a través de una comunicación procedente de fuentes externas, como investigadores de seguridad), debe compartir la información con los encargados del mantenimiento del producto con elementos digitales, de conformidad con su política de ciberseguridad. Los encargados del mantenimiento de los productos con elementos digitales o los administradores también deben valorar la posibilidad de notificar la vulnerabilidad de forma voluntaria, de conformidad con el artículo 15.

81. Por otra parte, cuando un administrador proporcione la infraestructura informática subyacente para determinados productos con elementos digitales, está obligado a notificar a la ENISA y a los CSIRT, de conformidad con el artículo 14, apartado 3, los incidentes graves relacionados con dicha infraestructura que repercutan en la seguridad de los productos con elementos digitales. También está obligado, en su caso, a informar a todos los usuarios (por ejemplo, mediante un anuncio general). Como se ha indicado en el punto anterior, si bien el administrador no está obligado a notificar las vulnerabilidades aprovechadas activamente de las que tenga conocimiento, debe promover su correcta gestión y valorar la posibilidad de notificarlas de forma voluntaria de conformidad con el artículo 15.

82. Por último, cuando un administrador también proporcione recursos de ingeniería a productos con elementos digitales específicos, estará obligado a: i) notificar, de conformidad con el artículo 14, apartado 1, las vulnerabilidades aprovechadas activamente de las que tenga conocimiento; y ii) cuando proceda, informar a todos los usuarios. En la medida en que el administrador también tenga una relación directa con los usuarios afectados, está obligado asimismo a informarles directamente, de conformidad con el artículo 14, apartado 8.

83. Cuando una entidad deje de prestar apoyo sistemático de forma continuada a un programa informático libre y de código abierto específico, es posible que deje de cumplir los requisitos para considerarse «administrador» y, por tanto, que deje de estar sujeta a las obligaciones correspondientes. En tales casos, se recomienda a la entidad comunicar claramente el cambio en su condición con respecto a ese programa informático libre y de código abierto específico.

84. En determinadas situaciones, una entidad que haya sido administrador de un proyecto específico puede decidir monetizar dicho proyecto directamente, introduciendo así el producto con elementos digitales en el mercado y dando lugar a las obligaciones del fabricante en virtud del Reglamento de Ciberresiliencia. En tales circunstancias, dicha entidad se considerará fabricante del producto con elementos digitales a partir de la fecha en que lo introduce en el mercado (pero no en relación con las versiones anteriores respecto de las cuales actuara como administrador).

3.4. **Colaboradores y usos *downstream***

85. Como ya se ha indicado en la sección *3.1* Determinación de cuándo un programa informático libre y de código abierto se considera responsabilidad de una persona, el Reglamento de Ciberresiliencia aclara que no se aplicará a las «personas físicas o jurídicas que contribuyan con código fuente a productos con elementos digitales que se consideren programas informáticos libres y de código abierto que no estén bajo su responsabilidad» (considerando 18).

86. Los fabricantes de productos con elementos digitales que integran componentes de programas informáticos libres y de código abierto en sus propios productos con elementos digitales tampoco pasan a ser responsables de la conformidad de dichos componentes con el Reglamento de Ciberresiliencia, incluso cuando contribuyan con código fuente a su mantenimiento.

87. Del mismo modo, el mero hecho de que los fabricantes integren componentes de programas informáticos libres y de código abierto en sus propios productos con elementos digitales (monetizados) no afecta a la situación de dichos componentes de programas informáticos libres y de código abierto a efectos del Reglamento de Ciberresiliencia. Los encargados del mantenimiento de componentes de programas informáticos libres y de código abierto que no se introduzcan en el mercado no están sujetos a obligaciones en relación con otras entidades que puedan integrar dichos componentes en sus productos con elementos digitales. El hecho de que el Reglamento de Ciberresiliencia se aplique a un determinado componente de programas informáticos libres y de código abierto depende exclusivamente de si la persona física o jurídica que lo publica lo introduce en el mercado.

88. No obstante, los fabricantes de productos con elementos digitales que integren componentes de programas informáticos libres y de código abierto están obligados a cumplir el Reglamento de Ciberresiliencia en relación con sus propios productos con elementos digitales. También tienen una obligación de diligencia debida, de conformidad con el artículo 13, apartado 5, respecto de los componentes de programas informáticos libres y de código abierto que integren. Además, están obligados a notificar las vulnerabilidades de los componentes integrados y a compartir las correcciones de seguridad de conformidad con el artículo 13, apartado 6. Para obtener más información sobre esta cuestión, véase la sección *9.2.1* Notificación *upstream* y puesta en común de las correcciones de seguridad.

3.5. **Ejemplos ilustrativos**

89. Los ejemplos que figuran a continuación son completamente hipotéticos y tienen como única finalidad ilustrar los distintos casos expuestos en las secciones anteriores.

Ejemplo 27: el desarrollador independiente A ha desarrollado un programa informático libre y de código abierto. El desarrollador A publica dicho programa informático libre y de código abierto con su propio nombre o marca comercial, pero no cobra un precio por su uso. El programa informático se comparte abiertamente y está a disposición de todos de forma gratuita para que puedan acceder a él, utilizarlo, modificarlo y redistribuirlo. El desarrollador A también incluye un enlace a una plataforma para recaudar donaciones voluntarias.

Las empresas B, C y D integran dicho programa informático libre y de código abierto en sus propios productos con elementos digitales. Para apoyar el mantenimiento continuo, las empresas B, C y D realizan donaciones voluntarias al desarrollador A. Estas donaciones permiten al desarrollador A mantener el proyecto de forma activa.

No se considera que dicho programa informático libre y de código abierto se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia. El desarrollador A no tiene ninguna obligación en virtud del Reglamento de Ciberresiliencia. Las empresas B, C y D deben ejercer la diligencia debida de conformidad con el artículo 13, apartado 5, al integrar el programa informático libre y de código abierto en sus propios productos con elementos digitales.

Ejemplo 28: la fundación sin ánimo de lucro F publica un componente de un programa informático libre y de código abierto para integrarlo en otros productos comerciales con elementos digitales. La fundación F se compromete a prestar un apoyo continuado a dicho programa informático libre y de código abierto para garantizar su viabilidad y adopción. Las empresas A, B y C integran dicho programa informático libre y de código abierto en sus propios productos con elementos digitales. Las empresas A y B contribuyen voluntariamente con parte del tiempo de sus desarrolladores al desarrollo y mantenimiento de proyectos de programas informáticos libres y de código abierto en el seno de la fundación F, también para dicho programa informático libre y de código abierto.

Dado que la fundación F es una entidad sin ánimo de lucro creada de tal manera que sus ingresos después de los costes se utilizan para alcanzar objetivos sin ánimo de lucro, no se considera que el programa informático libre y de código abierto se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia. La fundación F es el administrador del programa informático libre y de código abierto y está sujeta a las obligaciones correspondientes establecidas en el artículo 24. Las empresas A, B y C deben ejercer la diligencia debida de conformidad con el artículo 13, apartado 5, al integrar el programa informático libre y de código abierto en sus propios productos con elementos digitales.

Ejemplo 29: la empresa A ha desarrollado un componente de programa informático libre y de código abierto para integrarlo en sus propios productos con elementos digitales. También publica este programa informático libre y de código abierto por separado con su propio nombre o marca comercial y lo mantiene de forma activa. Sin embargo, no cobra por su uso ni lo monetiza de otras maneras. Las empresas B, C y D integran dicho programa informático libre y de código abierto en sus propios productos con elementos digitales y contribuyen voluntariamente con parte del tiempo de sus desarrolladores a su mantenimiento.

No se considera que dicho programa informático libre y de código abierto se haya introducido en el mercado en el sentido del Reglamento de Ciberresiliencia. La empresa A no es su fabricante, sino su administrador. Las empresas B, C y D deben ejercer la diligencia debida de conformidad con el artículo 13, apartado 5, al integrar el programa informático libre y de código abierto en sus propios productos con elementos digitales.

Ejemplo 30: la empresa A publica un programa informático libre y de código abierto con su propio nombre o marca comercial y lo ofrece como versión de pago, que incluye determinadas prestaciones, como asistencia técnica u optimización del rendimiento. Los desarrolladores de las empresas B, C y D contribuyen al mantenimiento del programa informático libre y de código abierto, pero este sigue bajo el control de la empresa A.

Se considera que la empresa A es el fabricante del programa informático libre y de código abierto ([15]). Las empresas B, C y D no están sujetas a obligaciones en virtud del Reglamento de Ciberresiliencia en lo que respecta a dicho programa informático libre y de código abierto específico. Si integrasen dicho programa informático libre y de código abierto en sus propios productos con elementos digitales, entonces estarían obligados a ejercer la diligencia debida de conformidad con el artículo 13, apartado 5.

Ejemplo 31: la empresa A publica un programa informático libre y de código abierto con su propio nombre o marca comercial y proporciona mantenimiento continuo para garantizar su viabilidad a largo plazo, de tal manera que dicho programa informático pueda integrarse en los productos de otras empresas con elementos digitales. La empresa A no cobra por su uso, no trata los datos personales que recoge a través del producto con elementos digitales ni vende servicios de asistencia asociados a la publicación del programa informático libre y de código abierto.

La empresa B contribuye con código y tiempo de sus desarrolladores al mantenimiento del programa informático libre y de código abierto, pero no lo distribuye con fines comerciales. La empresa B ofrece servicios de asistencia técnica independientemente de la distribución del programa informático libre y de código abierto. Se considera que la empresa A es el administrador de dicho programa informático libre y de código abierto, mientras que la empresa B no está sujeta a ninguna obligación en virtud del Reglamento de Ciberresiliencia en lo que respecta al programa informático libre y de código abierto.

Ejemplo 32: una entidad sin ánimo de lucro creada de tal manera que garantiza que todos los ingresos después de los costes se utilizan para alcanzar objetivos sin ánimo de lucro publica un componente de programa informático libre y de código abierto. La entidad proporciona apoyo continuado para garantizar la viabilidad a largo plazo del proyecto. El mantenimiento se financia con fondos públicos, como subvenciones a la investigación. Los desarrollos adicionales, incluidas las nuevas funcionalidades, se financian mediante donaciones y proyectos específicos, realizados en colaboración con fabricantes que integran dicho programa informático libre y de código abierto en sus productos con elementos digitales. Estas funcionalidades se incorporan a la base de código del programa informático libre y de código abierto.

Se considera que la entidad sin ánimo de lucro que publica el programa informático libre y de código abierto es el administrador de dicho componente de programa informático. Un fabricante que ha contribuido al desarrollo de determinadas funcionalidades no se convierte en fabricante de dicho componente de programa informático libre y de código abierto. Cuando el fabricante integre dicho componente de programa informático libre y de código abierto en su propio producto con elementos digitales, deberá ejercer la diligencia debida de conformidad con el artículo 13, apartado 5.

Ejemplo 33: una entidad sin ánimo de lucro creada de tal manera que garantiza que todos los ingresos después de los costes se utilizan para alcanzar objetivos sin ánimo de lucro publica un kit de desarrollo de programas informáticos libre y de código abierto y garantiza su mantenimiento continuo. El kit de desarrollo se comparte abiertamente y está a disposición de todos de forma gratuita para que puedan acceder a él, utilizarlo, modificarlo y redistribuirlo. La financiación se obtiene a través de cuotas de afiliación que se abonan a la entidad sin ánimo de lucro, y los desarrolladores empleados por las organizaciones miembros contribuyen con código y otros recursos al desarrollo del kit de desarrollo de programas informáticos. Los fabricantes utilizan el kit de desarrollo como componente para crear otros productos con elementos digitales.

Se considera que la entidad sin ánimo de lucro que publica el kit de desarrollo es su administrador. Los miembros de la fundación no son responsables de la conformidad del kit de desarrollo con el Reglamento de Ciberresiliencia. Cuando haya fabricantes que utilicen el kit de desarrollo de programas informáticos para crear su propio producto con elementos digitales, deben ejercer la diligencia debida de conformidad con el artículo 13, apartado 5.

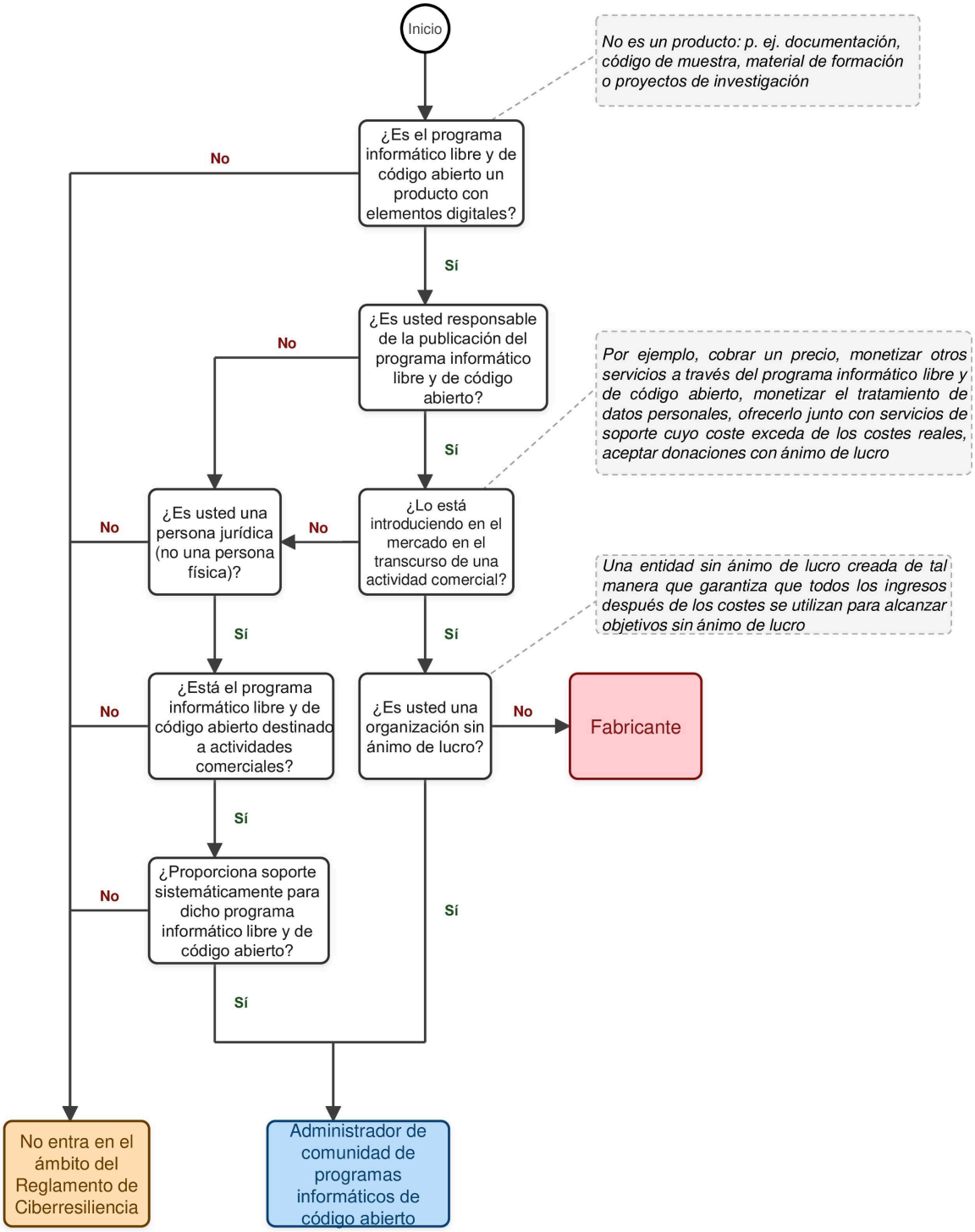
Ejemplo 34: un desarrollador independiente publica una biblioteca de programas informáticos libres y de código abierto en un repositorio público de paquetes para un determinado lenguaje de programación y la mantiene de forma activa. En la documentación del paquete, el desarrollador añade un enlace para recaudar donaciones. Un fabricante descarga de forma gratuita dicha biblioteca del repositorio y la integra en su propio producto con elementos digitales.

El desarrollador independiente y el repositorio de paquetes no están sujetos a ninguna obligación en virtud del Reglamento de Ciberresiliencia. El fabricante que integra la biblioteca debe ejercer la diligencia debida de conformidad con el artículo 13, apartado 5.

([15]) A menos que la empresa A sea una entidad sin ánimo de lucro creada de tal manera que garantice que todos los ingresos después de los costes se utilicen para alcanzar objetivos sin ánimo de lucro, en cuyo caso sería el administrador del programa informático libre y de código abierto.

Gráfico 1:

diagrama de flujo esquematizado sobre la aplicación del Reglamento de Ciberresiliencia a los programas informáticos libres y de código abierto



4. MODIFICACIONES SUSTANCIALES Y PIEZAS DE RECAMBIO

90. El artículo 3, punto 30, del Reglamento de Ciberresiliencia define «modificación sustancial» como un cambio en un producto con elementos digitales tras su introducción en el mercado que i) afecta al cumplimiento por parte del producto con elementos digitales de los requisitos esenciales establecidos en el anexo I, parte I; o ii) provoca la modificación de la finalidad prevista para la que se ha evaluado el producto con elementos digitales.

91. El concepto de «modificación sustancial» es pertinente para determinar las obligaciones derivadas del Reglamento de Ciberresiliencia en una serie de casos, entre ellos los siguientes:

a) de conformidad con el artículo 21, un importador o distribuidor que lleve a cabo una modificación sustancial de un producto con elementos digitales ya introducido en el mercado se considerará su fabricante;

b) de conformidad con el artículo 22, toda persona física o jurídica que lleve a cabo una modificación sustancial de un producto con elementos digitales y lo comercialice se considerará su fabricante;

c) de conformidad con el artículo 69, apartado 2, toda persona física o jurídica que lleve a cabo una modificación sustancial después del 11 de diciembre de 2027 de un producto con elementos digitales introducido en el mercado antes del 11 de diciembre de 2027 y lo introduzca en el mercado se considerará su fabricante;

d) en el caso de los fabricantes de productos con elementos digitales introducidos en el mercado después del 11 de diciembre de 2027, a fin de determinar si un producto con elementos digitales debe someterse a un nuevo procedimiento de evaluación de la conformidad debido a cambios realizados después de esa fecha, en particular a la luz del carácter iterativo del desarrollo de programas informáticos.

92. Por lo tanto, es importante proporcionar orientaciones para ayudar a los operadores económicos a comprender cuándo las modificaciones de equipos o programas informáticos se consideran modificaciones sustanciales.

4.1. **Reparaciones físicas**

93. Como se recoge en el considerando 42 del Reglamento de Ciberresiliencia, «[c]uando un producto con elementos digitales sea objeto de "reacondicionamiento", "mantenimiento" y "reparación", tal como se define en el artículo 2, puntos 18, 19 y 20, del Reglamento (UE) 2024/1781 del Parlamento Europeo y del Consejo, ello no conduce necesariamente a una modificación sustancial del producto, por ejemplo, si la finalidad prevista y las funcionalidades no se modifican y el nivel de riesgo no se ve afectado. No obstante, la mejora de un producto con elementos digitales por parte del fabricante podría dar lugar a cambios en el diseño y el desarrollo del producto y podría, por tanto, afectar a su finalidad prevista y a la conformidad con los requisitos establecidos en el presente Reglamento». Esto es coherente con la sección 2.1 de la Guía azul, que recuerda que «[u]n producto que ha sido objeto de cambios o revisiones importantes después de haber sido puesto en servicio debe ser considerado un producto nuevo si: i) se modifican sus prestaciones, su propósito o su tipo originales, sin que ello esté previsto en la evaluación inicial del riesgo; ii) la naturaleza del peligro ha cambiado o el nivel de riesgo ha aumentado en relación con la legislación de armonización de la Unión pertinente; y iii) el producto se comercializa (o se pone en servicio, si la legislación aplicable incluye también la puesta en servicio en su ámbito de aplicación). Este extremo debe ser evaluado de manera individual y, en especial, habida cuenta del objetivo de la legislación y del tipo de productos regulados por la legislación correspondiente».

94. Las operaciones de reacondicionamiento, mantenimiento o reparación que den lugar a modificaciones físicas de productos con elementos digitales ya introducidos en el mercado no constituyen necesariamente modificaciones sustanciales. Por tanto, debe realizarse una evaluación caso por caso para determinar si dicha modificación física afecta a la conformidad del producto con elementos digitales con los requisitos esenciales establecidos en la parte I del anexo I, o da lugar a un cambio en la finalidad prevista del producto contemplado en la evaluación de los riesgos de ciberseguridad.

95. La sustitución de piezas defectuosas o elementos usados por piezas de mejores prestaciones (por ejemplo, debido a los avances técnicos o porque la pieza antigua ya no se fabrica) no desencadena por sí sola una modificación sustancial del producto con elementos digitales reparado. Solo dará lugar a una modificación sustancial si el cambio en las prestaciones o la forma en que funciona el producto con elementos digitales reparado i) afecta a su conformidad con los requisitos esenciales o ii) da lugar a un cambio en la finalidad prevista que no estuviera contemplado en la evaluación de riesgos.

Ejemplo 35: el fabricante de un servidor realiza una operación de reparación, cambiando una RAM defectuosa por otra nueva y con mejores prestaciones. La conformidad con los requisitos esenciales por parte del servidor no se ve afectada. El servidor funciona mejor, pero sus nuevas prestaciones se mantienen dentro del uso previsto del servidor, tal como se tiene en cuenta en la evaluación de los riesgos de ciberseguridad. Por tanto, no se considera que el servidor se haya modificado sustancialmente.

4.2. **Piezas de recambio**

96. El artículo 2, apartado 6, del Reglamento de Ciberresiliencia establece que las piezas de recambio destinadas a reemplazar componentes idénticos y que se fabriquen con arreglo a las mismas especificaciones que dichos componentes no están sujetas al Reglamento. El considerando 29 establece además que la exención abarca tanto los repuestos para productos con elementos digitales comercializados antes de la fecha de aplicación del Reglamento, como los repuestos que ya se hayan sometido a un procedimiento de evaluación de la conformidad con arreglo al Reglamento.

97. La exención prevista en el artículo 2, apartado 6, del Reglamento de Ciberresiliencia debe entenderse en el sentido de que se aplica únicamente cuando la pieza de recambio se suministre específicamente para reparar o ampliar la durabilidad de un producto con elementos digitales ya introducido en el mercado (antes o después del 11 de diciembre de 2027). Cuando un producto con elementos digitales se suministra como producto independiente, sin ninguna relación con el mantenimiento o la reparación de un producto con elementos digitales preexistente, se introduce en el mercado en el sentido del Reglamento de Ciberresiliencia y no debe considerarse una pieza de recambio que entre en el ámbito de aplicación del artículo 2, apartado 6. La finalidad de mantenimiento o reparación debe quedar patente en el contexto del suministro, por ejemplo, mediante la identificación del producto con elementos digitales o la familia de productos en el pedido o en la oferta comercial, o mediante el suministro a través de canales posventa o de servicio. Asimismo, deben conservarse a disposición de las autoridades de vigilancia del mercado las pruebas que acrediten dicha finalidad. El hecho de que un producto con elementos digitales pueda utilizarse técnicamente para reemplazar un componente no es, por sí solo, suficiente para incluirlo en el ámbito de aplicación de la exención si no concurren tales circunstancias.

98. Así pues, cuando una pieza de recambio sea idéntica a un componente ya incluido en un producto con elementos digitales introducido en el mercado antes de la fecha de aplicación del Reglamento de Ciberresiliencia o que se haya introducido en el mercado de conformidad con dicho Reglamento, esa pieza de recambio no está sujeta al Reglamento de Ciberresiliencia.

99. La evaluación de si una pieza de recambio debe considerarse idéntica a un componente debe centrarse en su función en el producto con elementos digitales y en las características que puedan ser pertinentes para la ciberseguridad. Si bien siempre es necesaria una evaluación caso por caso, las diferencias que no afecten a las características de seguridad o al perfil de riesgo de ciberseguridad del componente no impiden, por sí solas, que dicha pieza de recambio entre en el ámbito de aplicación del artículo 2, apartado 6, del Reglamento de Ciberresiliencia.

100. En cambio, las diferencias en las características pertinentes para la ciberseguridad del componente, como algoritmos, protocolos, mecanismos criptográficos, funciones de control de acceso u otras características pertinentes para la seguridad, pueden hacer que la nueva pieza pueda no considerarse idéntica al componente al que está destinada a reemplazar.

101. Cuando una pieza de recambio no es idéntica al componente original, constituye por sí sola un producto con elementos digitales y, por tanto, está sujeta al Reglamento de Ciberresiliencia. En tales casos, el cumplimiento de los requisitos esenciales debe evaluarse a la luz de la finalidad prevista del componente de sustitución. Reviste especial importancia la función del componente de sustitución de garantizar la compatibilidad o la interoperabilidad con un producto con elementos digitales existente, en particular cuando dicho producto sea un producto con elementos digitales introducido en el mercado antes de fecha de aplicación del Reglamento de Ciberresiliencia. Cuando determinados requisitos esenciales no puedan cumplirse razonablemente debido a dicha finalidad prevista o a limitaciones técnicas, el fabricante deberá reflejarlo en la evaluación de los riesgos de ciberseguridad y aplicar medidas alternativas o compensatorias adecuadas de reducción del riesgo, a fin de no socavar la seguridad del producto con elementos digitales. Como se analiza también en la sección *2.6* Sistemas complejos, tanto la documentación técnica como la información y las instrucciones para el usuario desempeñan un papel fundamental a la hora de describir de manera transparente las limitaciones detectadas, los riesgos de ciberseguridad asociados y las medidas de reducción del riesgo aplicadas. Como se explica en la sección *4.1* Reparaciones físicas, la sustitución de piezas defectuosas o elementos usados por piezas de mejores prestaciones no desencadena por sí sola una modificación sustancial del producto con elementos digitales reparado.

Ejemplo 36: un fabricante ha introducido en el mercado de la UE controladores conectados. En un caso, el controlador se introdujo en el mercado en 2026, antes de la fecha de aplicación del Reglamento de Ciberresiliencia. En otro caso, el controlador se introdujo en el mercado en 2028, de conformidad con el Reglamento de Ciberresiliencia. En 2028, falla un módulo de comunicación digital en ambos tipos de controladores. El fabricante suministra como pieza de recambio un módulo de sustitución idéntico al original y fabricado conforme a las mismas especificaciones.

En ambos casos, el módulo de sustitución entra en el ámbito de aplicación de la exención del artículo 2, apartado 6. La pieza de recambio por sí sola no está sujeta al Reglamento de Ciberresiliencia, aunque se trate de un producto con elementos digitales, ya que reemplaza a un componente idéntico de un producto con elementos digitales. La reparación no constituye una modificación sustancial del producto con elementos digitales.

Ejemplo 37: en 2026, un fabricante introdujo en el mercado de la UE un controlador industrial conectado, antes de la fecha de aplicación del Reglamento de Ciberresiliencia. En 2028, falla un chip de comunicación de dicho controlador. Dado que el fabricante ya no fabrica ese chip, suministra como pieza de recambio un chip más moderno con una funcionalidad equivalente, pero con una implementación criptográfica diferente y un mecanismo de arranque seguro actualizado, con el fin de mantener la compatibilidad y el funcionamiento continuado.

En este caso, el chip de sustitución no puede considerarse idéntico, ya que las diferencias en la implementación criptográfica y el mecanismo de arranque seguro afectan a las características de ciberseguridad del chip. Por lo tanto, no se beneficia de la exención prevista en el artículo 2, apartado 6, y constituye un producto con elementos digitales sujeto al Reglamento de Ciberresiliencia. La conformidad de la pieza de sustitución debe evaluarse a la luz de su finalidad prevista, incluida su función de garantizar la interoperabilidad con el producto con elementos digitales introducido en el mercado antes de la fecha de aplicación del Reglamento de Ciberresiliencia.

Ejemplo 38: en 2028, un fabricante introduce en el mercado un controlador de edificios inteligentes de conformidad con el Reglamento de Ciberresiliencia. En 2029, falla el módulo inalámbrico de dicho controlador. Dado que el fabricante ya no fabrica ese módulo, suministra como pieza de recambio un módulo nuevo que desempeña la misma función utilizando los mismos protocolos de comunicación y mecanismos de seguridad, pero se basa en un conjunto de chips diferente y cuenta con un firmware *actualizado que no altera características que puedan ser pertinentes para la ciberseguridad.*

En este caso, el módulo de sustitución puede considerarse idéntico. Por lo tanto, el módulo se beneficia de la exención prevista en el artículo 2, apartado 6, y no está sujeto al Reglamento de Ciberresiliencia.

102. La exención para las piezas de recambio se aplica con independencia de que la pieza reemplace a un componente de un producto con elementos digitales o a un producto con elementos digitales completo que, a su vez, forme parte de un producto de mayor tamaño, incluso cuando dicho producto con elementos digitales de mayor tamaño esté formado por varios componentes integrados, siempre que la pieza de sustitución se suministre específicamente como pieza de recambio, tal como se explica en los apartados anteriores.

Ejemplo 39: en 2027, un fabricante comercializa un sistema de automatización industrial que incorpora un controlador lógico programable como uno de sus componentes. En 2031, falla la unidad central de procesamiento (UCP) del controlador lógico programable. El fabricante ofrece dos opciones de reparación: i) suministrar una UCP de sustitución, que pueda considerarse idéntica a la UCP instalada originalmente; o ii) suministrar un controlador lógico programable completo de sustitución, que pueda considerarse idéntico al controlador lógico programable instalado originalmente. En cada caso, la sustitución se facilita a través del canal de servicio posventa del fabricante como pieza de recambio, y el sistema de automatización industrial para el que está destinada la pieza de sustitución está claramente identificado. En ambos casos, la pieza de sustitución entra en el ámbito de aplicación de la exención prevista en el artículo 2, apartado 6, tanto si la sustitución se refiere a un componente del controlador lógico programable como si se refiere al controlador lógico programable en su conjunto.

4.3. **Actualizaciones de programas informáticos como modificaciones sustanciales**

103. El desarrollo de programas informáticos tiene un carácter iterativo, y los productos con elementos digitales consistentes en programas informáticos ya introducidos en el mercado se actualizan con frecuencia y de forma continua. En este contexto, conviene proporcionar más orientaciones para determinar cuándo debe considerarse que el programa informático ha sido objeto de una modificación sustancial. Estas orientaciones tienen por objeto, en particular, ayudar a los fabricantes de productos con elementos digitales consistentes en programas informáticos que realizan cambios en sus propios productos a determinar si dichos cambios constituyen una modificación sustancial.

104. El considerando 39 indica que un producto con elementos digitales se modifica sustancialmente cuando un cambio altera el nivel de riesgo de ciberseguridad y cuando el fabricante no ha tenido en cuenta dicho riesgo nuevo o adicional en su evaluación de riesgos ni, por consiguiente, en su aplicación de los requisitos esenciales. Por lo tanto, un fabricante debe evaluar, caso por caso, si la actualización de un programa informático introduce riesgos de ciberseguridad nuevos o mayores, y si dichos riesgos ya se han abordado en su evaluación de riesgos.

105. Cuando un fabricante introduce nuevas funcionalidades en un producto con elementos digitales que dan lugar a un cambio en la finalidad prevista del producto en su conjunto, es probable que el fabricante no haya tenido en cuenta dichos cambios en su evaluación de riesgos. En estas circunstancias, el cambio constituiría por lo general una modificación sustancial.

Ejemplo 40: un fabricante introduce en el mercado un panel de control que recoge datos de máquinas y muestra tendencias y alertas, sin tener capacidad para controlar dichas máquinas. A continuación, el fabricante desarrolla una nueva versión de dicho panel de control, introduciendo funcionalidades que le permiten controlar las máquinas, en particular ajustando los parámetros de funcionamiento y reiniciando las máquinas tras situaciones de fallo. Como consecuencia de estos cambios, la finalidad prevista del panel de control ha evolucionado más allá de lo previsto en la evaluación de riesgos, y ha pasado de ser una herramienta de conciencia situacional a ser un producto con elementos digitales destinado a ejercer control operativo sobre otros dispositivos. Por lo tanto, el panel de control ha sido objeto de una modificación sustancial.

Ejemplo 41: un fabricante introduce en el mercado una aplicación de programa informático destinada a consumidores cuya finalidad es organizar y mostrar datos personales, como correos electrónicos, mensajes o documentos, y ofrecer funciones básicas de búsqueda y filtrado. Posteriormente, el fabricante introduce una actualización que permite que la aplicación analice automáticamente el contenido de los usuarios con el fin de generar perfiles de comportamiento y tomar decisiones automatizadas que afectan a la priorización, supresión o recomendación de contenidos sin intervención del usuario. Como consecuencia de este cambio, la finalidad prevista del programa informático pasa de ser una herramienta de gestión de la información bajo el control del usuario a ser un sistema de toma de decisiones automatizada, lo que no se había contemplado en la evaluación de riesgos. Por lo tanto, la aplicación ha sido objeto de una modificación sustancial.

106. Al mismo tiempo, sin embargo, es posible que un fabricante introduzca progresivamente nuevas funcionalidades ya incluidas en su evaluación de riesgos o que, por sí mismas, no alteran el perfil de riesgo de ciberseguridad del producto con elementos digitales. Este puede ser el caso, por ejemplo, cuando el fabricante haya previsto el desarrollo de dichas funcionalidades, haya descrito y evaluado ya los riesgos asociados y haya aplicado medidas de mitigación adecuadas para garantizar el cumplimiento continuado de los requisitos esenciales. Este puede ser también el caso cuando las nuevas funcionalidades no introduzcan cambios que den lugar a riesgos nuevos o mayores. Por lo tanto, las actualizaciones de esta naturaleza no deben considerarse modificaciones sustanciales, ya que no aumentan el riesgo de ciberseguridad y, en consecuencia, no alteran la aplicación de los requisitos esenciales.

Ejemplo 42: una aplicación de mensajería se lanza inicialmente con una funcionalidad limitada a la mensajería individual. La evaluación de riesgos del fabricante contempla la introducción posterior de la mensajería en grupo, incluida, por ejemplo, la mayor complejidad del enrutamiento de mensajes. En una actualización posterior, el fabricante añade una funcionalidad de chat grupal junto con controles de administrador y herramientas de moderación que ya se habían previsto y evaluado en el diseño original. La actualización incorpora funcionalidades que entran en el ámbito de la finalidad prevista y la evaluación de riesgos originales. Por lo tanto, la aplicación de mensajería no ha sido objeto de una modificación sustancial.

Ejemplo 43: se introduce en el mercado un sistema de supervisión de la producción con paneles de control habilitados únicamente para la consulta de datos, mientras que en la arquitectura del sistema hay presentes funciones de control automatizado, pero que permanecen desactivadas. La evaluación de riesgos del fabricante contempla expresamente la futura activación de los circuitos de control automatizado, incluidos los riesgos de ciberseguridad asociados al control en bucle cerrado, así como salvaguardias como mecanismos de anulación por parte del operador y estados de seguridad a prueba de fallos. En una actualización posterior, el fabricante habilita las funciones de control automatizado y activa las salvaguardias tal como se habían evaluado inicialmente. Por lo tanto, el sistema de supervisión de la producción no ha sido objeto de una modificación sustancial.

107. Por el contrario, incluso las funcionalidades nuevas limitadas o aparentemente menores pueden introducir riesgos de ciberseguridad significativos que afecten a la conformidad con los requisitos esenciales. Por lo tanto, la evaluación de la modificación sustancial no debe basarse en la magnitud o la complejidad del cambio, sino en sus posibles efectos adversos en el perfil de riesgo de ciberseguridad del producto con elementos digitales y, por consiguiente, en la aplicación de los requisitos esenciales.

Ejemplo 44: un fabricante introduce una actualización en una aplicación informática que añade una función de «recuérdame» o de inicio de sesión persistente que almacena localmente testigos de autenticación para facilitar su uso por parte del usuario. Aunque la funcionalidad tiene un alcance limitado, introduce nuevos riesgos relacionados con el robo de testigos de autenticación, el acceso no autorizado y el secuestro de sesiones que no se habían tenido en cuenta en la evaluación de riesgos. Por lo tanto, la actualización afecta a la conformidad con los requisitos esenciales. Así pues, la aplicación informática ha sido objeto de una modificación sustancial.

Ejemplo 45: un fabricante añade una nueva función de registro y diagnóstico a un producto existente con elementos digitales consistente en un programa informático, que permite exportar registros detallados del sistema con fines de resolución de problemas. Si bien la funcionalidad parece menor, da lugar a la recogida y el almacenamiento de datos operativos sensibles en un formato no cifrado, lo que introduce riesgos de exposición de los datos que no se habían evaluado ni mitigado anteriormente. Por lo tanto, el cambio puede tener un impacto significativo en el perfil de riesgo de ciberseguridad del producto con elementos digitales. El producto con elementos digitales consistente en un programa informático ha sido objeto de una modificación sustancial.

108. En consonancia con el considerando 39 del Reglamento de Ciberresiliencia, las actualizaciones de seguridad no deben considerarse, por lo general, modificaciones sustanciales, ya que su objetivo principal es reducir el nivel de riesgo de ciberseguridad asociado al producto con elementos digitales. Por lo tanto, una actualización de seguridad que no modifique la finalidad prevista de dicho producto y no introduzca nuevos riesgos de ciberseguridad no debe considerarse una modificación sustancial, aun cuando dicha actualización pueda introducir cambios técnicos significativos. Esto incluye los casos en los que determinadas funcionalidades se modifican o limitan únicamente con el fin de mitigar las vulnerabilidades detectadas y garantizar el cumplimiento continuado de los requisitos esenciales.

Ejemplo 46: un fabricante implementa una actualización de seguridad para abordar una vulnerabilidad en la base de código de un producto con elementos digitales, ya sea corrigiendo un error de validación de entradas que podría dar lugar a un desbordamiento de búfer o subsanando un fallo lógico que permitiría eludir la autenticación debido a una validación incorrecta de los testigos de autenticación de sesión. La actualización modifica la implementación interna del programa informático sin afectar a la finalidad prevista de dicho producto ni introducir una nueva exposición. Dicha actualización tiene como única finalidad reducir el riesgo de ciberseguridad. La actualización de seguridad no debe considerarse una modificación sustancial.

Ejemplo 47: un fabricante introduce una actualización de seguridad que refuerza las configuraciones de seguridad existentes, por ejemplo, endureciendo las reglas del cortafuegos, deshabilitando los puertos de red no utilizados, modificando las políticas de contraseña predeterminada del administrador o haciendo obligatoria la autenticación multifactor, si dicha funcionalidad ya estaba disponible o prevista. Aunque la actualización puede afectar a la forma en que los usuarios configuran el producto con elementos digitales o acceden a él, no altera su finalidad prevista y sirve exclusivamente para mejorar su nivel de seguridad. La actualización de seguridad no debe considerarse una modificación sustancial.

Ejemplo 48: un fabricante introduce en el mercado un producto con elementos digitales consistente en un programa informático que protege las comunicaciones utilizando un marco de cifrado configurable compatible con múltiples algoritmos criptográficos y tamaños de clave, tal como se describe en la documentación técnica y la evaluación de riesgos del producto. La evaluación de riesgos contempla todas las opciones criptográficas que ofrece el producto con elementos digitales y anticipa la futura deprecación de determinados algoritmos. La evaluación de riesgos también incluye medidas de mitigación, como la agilidad criptográfica, la gestión interna de claves y las pruebas de compatibilidad. En respuesta a las nuevas orientaciones criptográficas, el fabricante implementa una actualización de seguridad que inhabilita un algoritmo deprecado y activa una alternativa más sólida ya compatible con el producto, sin introducir nuevas dependencias externas ni alterar los flujos de datos. Dado que la actualización aplica una medida de seguridad ya prevista y evaluada como parte del diseño original, y no introduce nuevos riesgos de ciberseguridad, la actualización de seguridad no debe considerarse una modificación sustancial.

109. En cambio, una actualización de seguridad puede constituir una modificación sustancial cuando, pese a su finalidad de seguridad, la actualización modifica la finalidad prevista del producto con elementos digitales más allá de lo contemplado inicialmente o introduce riesgos de ciberseguridad nuevos o mayores. Este puede ser el caso, por ejemplo, cuando una actualización modifica sustancialmente los límites o la estructura de dependencias de dicho producto de una manera no prevista en la evaluación de riesgos, por ejemplo, al alterar sustancialmente los flujos de datos o al añadir nuevas interfaces accesibles desde el exterior.

Ejemplo 49: un fabricante introduce en el mercado un producto con elementos digitales consistente en un programa informático destinado a proporcionar cifrado local de archivos para los datos almacenados en el dispositivo de un usuario, lo que permite a los usuarios cifrar y descifrar archivos cuando lo soliciten. Tras detectar una vulnerabilidad en el flujo de trabajo de cifrado, el fabricante implementa una actualización de seguridad que elimina la funcionalidad de cifrado local y, en su lugar, exige que todos los archivos se carguen, almacenen y procesen en un servicio de cifrado remoto gestionado por el fabricante. Como consecuencia de este cambio, el producto con elementos digitales ya no realiza el cifrado local previsto inicialmente y pasa a funcionar como un servicio de cifrado y tratamiento de datos a distancia. Aunque la actualización se introduce por razones de seguridad, modifica fundamentalmente la finalidad prevista de dicho producto de una manera no contemplada en la evaluación de riesgos, por lo que constituye una modificación sustancial.

Ejemplo 50: un fabricante introduce en el mercado un producto con elementos digitales consistente en un programa informático que se basa en un protocolo de cifrado establecido y en un ciclo de vida de las claves gestionado internamente para garantizar las comunicaciones entre los componentes del producto con elementos digitales. En respuesta a nuevas vulnerabilidades criptográficas detectadas, el fabricante introduce una actualización de seguridad que sustituye el mecanismo de cifrado existente por un protocolo diferente que requiere el uso de un servicio externo de gestión de claves gestionado por un tercero. Como consecuencia de este cambio, las dependencias y los flujos de datos del producto con elementos digitales se ven alterados de manera significativa, al introducir nuevas interfaces externas y una dependencia de servicios de terceros que no se habían contemplado en la evaluación de riesgos. Aunque la actualización responde a cuestiones de seguridad, introduce nuevos riesgos de ciberseguridad, por lo que constituye una modificación sustancial.

110. Como se ha indicado en el punto 104, la cuestión de si la actualización de un programa informático constituye una modificación sustancial debe evaluarse caso por caso. Al llevar a cabo dicha evaluación, los fabricantes podrían valorar, de manera no exhaustiva, si la actualización del programa informático:

a) introduce nuevos vectores de amenaza, como interfaces, canales de comunicación, entornos de ejecución o dependencias externas adicionales a través de los cuales podrían materializarse amenazas;

b) permite nuevos escenarios de ataque, incluidas, por ejemplo, nuevas formas en las que pudieran producirse de manera plausible accesos no autorizados, manipulaciones, interferencias o usos indebidos del producto con elementos digitales o de los datos tratados por este;

c) modifica la probabilidad de los escenarios de ataque determinados anteriormente, por ejemplo, al reducir el esfuerzo o los conocimientos especializados necesarios para explotarlos, aumentar la exposición a agentes que no son de confianza o debilitar las salvaguardias existentes;

d) modifica el posible impacto de los escenarios de ataque determinados anteriormente, incluidos, por ejemplo, el alcance de los datos o funciones afectados, la gravedad de las consecuencias operativas, económicas o de seguridad, o la capacidad para detectar, contener o subsanar un incidente.

111. En algunos casos, una actualización de un programa informático no introduce nuevos vectores de amenaza, no permite nuevos escenarios de ataque ni modifica sustancialmente la probabilidad o el impacto de los escenarios de ataque determinados anteriormente. Esto puede indicar que la actualización no introduce riesgos de ciberseguridad nuevos o mayores, siempre que las hipótesis y las medidas de mitigación en las que se basa la evaluación de riesgos sigan siendo válidas y eficaces. Por lo tanto, es probable que la actualización no constituya una modificación sustancial.

112. Por el contrario, una actualización de un programa informático puede introducir nuevos vectores de amenaza, permitir nuevos escenarios de ataque o alterar de manera significativa la probabilidad o el impacto de escenarios de ataque existentes. En tales casos, el fabricante debe volver a evaluar los riesgos de ciberseguridad del producto con elementos digitales y determinar si siguen cumpliéndose los requisitos esenciales, en particular si la actualización introduce riesgos nuevos o mayores no contemplados en la evaluación de riesgos.

113. Establecer si la actualización de un programa informático constituye una modificación sustancial es pertinente para comprobar si se aplican determinadas obligaciones en virtud del Reglamento de Ciberresiliencia, como se expone en el punto 91. Sin embargo, con independencia de que se consideren o no modificaciones sustanciales, los fabricantes siguen siendo responsables de garantizar la seguridad de las actualizaciones de los programas informáticos y de su producto con elementos digitales durante el período de soporte, de conformidad con los requisitos de gestión de las vulnerabilidades establecidos en la parte II del anexo I del Reglamento de Ciberresiliencia. Además, independientemente de que las actualizaciones de los programas informáticos constituyan o no modificaciones sustanciales, los fabricantes están obligados a mantener la evaluación del riesgo y la documentación técnica exactas y completas y permanentemente actualizadas, de conformidad con el artículo 13, apartado 7, y el artículo 31, apartado 2.

4.4. **Consecuencias de una modificación sustancial**

114. Las consecuencias de una modificación sustancial realizada por un agente distinto del fabricante original de un producto con elementos digitales ya introducido en el mercado se abordan en los artículos 21 y 22 del Reglamento de Ciberresiliencia. El artículo 21 se refiere a los importadores y distribuidores, mientras que el artículo 22 se refiere a cualquier persona física o jurídica distinta del fabricante, el importador o el distribuidor.

115. Cuando la modificación sustancial la realice el fabricante original del producto con elementos digitales, las consecuencias se derivan del concepto generalmente establecido de modificación sustancial a que se refiere el considerando 41 del Reglamento de Ciberresiliencia y que se desarrolla con más detalle en la sección 2.1 de la Guía azul. En dicha sección se establece que un producto que ha sido objeto de cambios o de revisiones importantes tras su introducción en el mercado debe considerarse un producto nuevo cuando se hayan modificado sus prestaciones, su propósito o su o tipo originales, cuando haya cambiado la naturaleza del peligro o haya aumentado el nivel de riesgo, y el producto con elementos digitales se comercialice.

116. Por lo tanto, la consecuencia generalmente establecida es que, cuando la modificación de un producto con elementos digitales constituye una modificación sustancial y el producto con elementos digitales modificado se comercializa, este debe tratarse, a efectos del Reglamento de Ciberresiliencia, como un producto con elementos digitales nuevo. En consecuencia, el acto de comercializar el producto sustancialmente modificado constituye una nueva introducción en el mercado. Esto se aplica tanto si la modificación sustancial la realiza el fabricante original como si la realiza otra persona. Con el fin de garantizar que el Reglamento de Ciberresiliencia se aplique de manera uniforme y proporcionada a las distintas categorías de agentes que pueden realizar una modificación sustancial, las subsecciones siguientes abordan las obligaciones resultantes para la persona que realiza la modificación sustancial cuando el producto con elementos digitales modificado sustancialmente se introduce en el mercado. Las consecuencias para el período de soporte del producto con elementos digitales se abordan en la sección 5 Período de soporte.

4.4.1. *Modificaciones sustanciales realizadas por una persona distinta del fabricante original*

117. De conformidad con los artículos 21 y 22, cuando una persona física o jurídica distinta del fabricante de un producto con elementos digitales realiza una modificación sustancial de dicho producto con elementos digitales ya introducido en el mercado, la persona que realiza la modificación sustancial y comercializa el producto modificado con elementos digitales debe considerarse el fabricante del producto modificado, con independencia de que participara o no en el diseño original o en la introducción en el mercado de dicho producto.

118. El artículo 22 aclara además que la persona que realiza la modificación está sujeta a las obligaciones establecidas en los artículos 13 y 14 únicamente en lo que respecta a la parte del producto con elementos digitales afectada por la modificación sustancial, siempre que dicha modificación no afecte a la ciberseguridad del producto con elementos digitales en su conjunto.

119. Cuando una modificación sustancial afecte a la conformidad con los requisitos esenciales, pero no afecte negativamente a la ciberseguridad del producto con elementos digitales en su conjunto, la persona que realice la modificación estará sujeta a lo dispuesto en los artículos 13 (en particular a la obligación de garantizar la conformidad con los requisitos esenciales y de llevar a cabo un procedimiento de evaluación de la conformidad) y 14 (obligaciones de información), únicamente en lo que respecta a la parte del producto con elementos digitales que haya sido modificada sustancialmente ([16]). Además, las obligaciones del fabricante original en virtud del Reglamento de Ciberresiliencia siguen aplicándose al producto con elementos digitales original introducido en el mercado, garantizando la continuidad de la gestión de las vulnerabilidades y de la conformidad respecto de las partes que no se hayan modificado.

120. Un caso de modificación sustancial no debe confundirse con los casos de integración, en los que una persona ensambla componentes (incluida, cuando proceda, su modificación) en un nuevo producto con elementos digitales que ella misma introduce en el mercado. En tales casos, el integrador no está modificando un producto con elementos digitales ya introducido en el mercado por otro fabricante, sino que está introduciendo en el mercado un nuevo producto con elementos digitales propio. A efectos del Reglamento de Ciberresiliencia, el integrador es el fabricante de ese nuevo producto con elementos digitales, y está obligado a cumplir íntegramente el Reglamento en relación con el producto con elementos digitales en su conjunto. Cuando el fabricante integre componentes sujetos al Reglamento de Ciberresiliencia, podrá basarse en las actividades de conformidad de los fabricantes de dichos componentes para facilitar su propio cumplimiento del Reglamento de Ciberresiliencia.

Ejemplo 51: una empresa adquiere módulos de microcontroladores y componentes de conectividad disponibles en el mercado de proveedores terceros, desarrolla un firmware *propio y un conjunto de sensores, y los ensambla en un producto de supervisión agrícola conectado con elementos digitales que introduce en el mercado bajo su propio nombre. Aunque la empresa ha modificado los módulos de microcontroladores subyacentes y los ha combinado con otros componentes, no está modificando sustancialmente un producto con elementos digitales ya introducido en el mercado, sino que está introduciendo en el mercado un nuevo producto con elementos digitales. A efectos del Reglamento de Ciberresiliencia, la empresa es el fabricante del sistema de supervisión agrícola, y está obligada a cumplir el Reglamento en relación con el sistema de supervisión agrícola en su conjunto.*

([16]) En consonancia con la sección 2.1 de la Guía Azul, «[n]o es necesario repetir los ensayos y elaborar nueva documentación relativa a los aspectos no afectados por la modificación. Corresponde a la persona física o jurídica que efectúa los cambios o que encarga los cambios en el producto demostrar que no es necesario actualizar todos los elementos de la documentación técnica. La persona física o jurídica que efectúa los cambios o que encarga los cambios en el producto será responsable de la conformidad del producto modificado y redactará una declaración de conformidad, incluso si utiliza los ensayos y la documentación técnica existentes».

121. Cuando una modificación sustancial realizada por una persona distinta del fabricante original afecte negativamente a la ciberseguridad del producto con elementos digitales en su conjunto, por ejemplo, porque la modificación ya no se limita a un componente o subsistema específico, el producto con elementos digitales modificado comercializado debe tratarse como un nuevo producto con elementos digitales sujeto al Reglamento de Ciberresiliencia en su totalidad. En tales casos, el perfil de riesgo de ciberseguridad global del producto ha cambiado y la modificación no puede evaluarse sin tener en cuenta el producto con elementos digitales en su conjunto. La persona que realiza la modificación está sujeta a las obligaciones del fabricante establecidas en los artículos 13 y 14 en relación con el producto con elementos digitales modificado en su conjunto.

4.4.2. *Modificaciones sustanciales realizadas por el fabricante original*

122. Cuando la modificación sustancial la realice el fabricante original, también en el contexto del desarrollo iterativo de productos con elementos digitales consistentes en programas informáticos, dicho fabricante seguirá siendo el fabricante a efectos del Reglamento de Ciberresiliencia. Sin embargo, el producto con elementos digitales sustancialmente modificado deberá considerarse un producto nuevo introducido en el mercado.

123. De conformidad con la sección 2.1 de la Guía azul, el fabricante original que introduzca en el mercado el producto con elementos digitales sustancialmente modificado podrá reutilizar la documentación y los ensayos existentes para aspectos del producto con elementos digitales que no se vean afectados por la modificación sustancial. En particular, cuando el fabricante introduzca en el mercado versiones sustancialmente modificadas del mismo producto con elementos digitales, el procedimiento de evaluación de la conformidad deberá centrarse en las partes del producto con elementos digitales que hayan sido sustancialmente modificadas. Del mismo modo, cuando se lleve a cabo una evaluación de la conformidad por terceros, el organismo de evaluación de la conformidad debe centrar su evaluación en las partes sustancialmente modificadas. En lo que respecta a las partes no modificadas del producto con elementos digitales, podrá reutilizar la documentación y los resultados de los ensayos existentes.

124. Las consideraciones de proporcionalidad expuestas en la subsección anterior se aplican igualmente a las modificaciones sustanciales realizadas por el fabricante original de un producto con elementos digitales introducido en el mercado antes del 11 de diciembre de 2027. Dicha modificación sustancial realizada por el fabricante original no lo obliga, por sí sola, a garantizar la plena conformidad con el Reglamento de Ciberresiliencia de la totalidad del producto con elementos digitales introducido en el mercado antes de esa fecha, a menos que la modificación afecte negativamente a la ciberseguridad del producto con elementos digitales en su conjunto. Cuando la modificación no afecte a la ciberseguridad del producto con elementos digitales en su conjunto, las obligaciones del fabricante original con respecto a la modificación deben limitarse a las partes sustancialmente modificadas.

5. **PERÍODO DE SOPORTE**

125. El artículo 13, apartado 8, del Reglamento de Ciberresiliencia exige a los fabricantes determinar el período de soporte durante el cual las vulnerabilidades del producto con elementos digitales, incluidos sus componentes, se gestionarán de manera eficaz y de conformidad con los requisitos esenciales establecidos en la parte II del anexo I. El período de soporte refleja el tiempo durante el cual se prevé que vaya a utilizarse el producto con elementos digitales (el período de uso previsto) y debe determinarse a la luz de los criterios establecidos en el artículo 13, apartado 8, en particular, las expectativas razonables de los usuarios, la naturaleza del producto con elementos digitales, incluida su finalidad prevista, así como las disposiciones pertinentes del Derecho de la Unión que determinen la vida útil de los productos con elementos digitales ([17]). En conjunto, estos criterios deben tenerse en cuenta de tal manera que se garantice la proporcionalidad a la hora de determinar el período de soporte.

([17]) Otros criterios adicionales que pueden tenerse en cuenta, de conformidad con el artículo 13, apartado 8, incluyen los períodos de soporte de productos con elementos digitales que ofrezcan una funcionalidad similar introducidos en el mercado por otros fabricantes, la disponibilidad del entorno operativo y los períodos de soporte de los componentes integrados que proporcionan las funciones principales y se obtienen de terceros, así como las orientaciones pertinentes facilitadas por el Grupo de Cooperación Administrativa (ADCO) y por la Comisión.

126. El artículo 13, apartado 8, exige además que el período de soporte sea de al menos cinco años, a menos que se prevea que el producto con elementos digitales vaya a utilizarse durante menos de cinco años, en cuyo caso el período de soporte corresponderá al tiempo de utilización previsto. Por lo tanto, el período mínimo de soporte actúa únicamente como salvaguardia, garantizando que las vulnerabilidades se gestionen durante un período suficientemente prolongado, al tiempo que permite a los fabricantes tener en cuenta los productos con elementos digitales cuyo tiempo de utilización previsto sea realmente más corto. El considerando 60 ofrece más orientaciones a este respecto y aclara que los productos con elementos digitales de los que quepa esperar razonablemente que se utilicen durante más de cinco años deben tener, en consecuencia, períodos de soporte más largos. Por lo tanto, un período de soporte de cinco años no debe considerarse el período por defecto para todos los productos con elementos digitales. En su lugar, el fabricante debe determinar el período de soporte adecuado a la luz de los criterios a que se refiere el artículo 13, apartado 8.

127. El artículo 13, apartado 19, exige a los fabricantes que indiquen en el momento de la compra, de manera clara y comprensible, la fecha final del período de soporte (al menos el mes y el año). Asimismo, exige a los fabricantes que muestren una notificación a los usuarios una vez que expire el período de soporte, cuando sea técnicamente viable teniendo en cuenta la naturaleza del producto con elementos digitales. Esta obligación tiene por objeto ofrecer transparencia a los usuarios en lo que respecta a la duración durante la cual pueden esperar recibir soporte en materia de seguridad.

128. En el caso de los productos con elementos digitales consistentes en programas informáticos, que a menudo se desarrollan y publican de forma iterativa y cuyas versiones sustancialmente modificadas pueden introducirse en el mercado con frecuencia a lo largo del tiempo, el período de soporte debe entenderse teniendo en cuenta este modelo de desarrollo. Cada versión sustancialmente modificada de un producto con elementos digitales consistente en un programa informático introducido en el mercado debe tener un período de soporte declarado que se ajuste a lo dispuesto en el artículo 13, apartado 8. Esto incluye el período mínimo de soporte de al menos cinco años, a menos que pueda demostrarse que el tiempo de utilización previsto de dicha versión es inferior a cinco años, como también se aclara en el considerando 60. La sección *5.1* Modificaciones sustanciales y período de soporte aclara además que, cuando la modificación sustancial no dé lugar a cambios en los factores que determinaron originalmente el tiempo de utilización previsto del producto con elementos digitales, el período de soporte original no se verá afectado (es decir, tampoco en los casos en que el período de soporte restante sea inferior a cinco años).

129. El artículo 13, apartado 10, ofrece flexibilidad para los productos con elementos digitales consistentes en programas informáticos al permitir a los fabricantes, en determinadas condiciones, garantizar el cumplimiento del requisito relativo a la gestión de las vulnerabilidades establecido en el punto 2 de la parte II del anexo I (responder a las vulnerabilidades y subsanarlas) únicamente para la última versión del producto con elementos digitales consistente en un programa informático que se haya introducido en el mercado. Esto está permitido cuando los usuarios de versiones introducidas anteriormente tienen acceso gratuito a la versión del producto introducida por última vez en el mercado y no incurren en costes adicionales para adaptar el entorno de equipos o programas informáticos en el que utilizan la versión anterior del producto en cuestión.

130. A efectos del artículo 13, apartado 10, el concepto de «costes adicionales» debe interpretarse de forma práctica y proporcionada, teniendo en cuenta las prácticas habituales y previsibles en el mantenimiento y el funcionamiento de los programas informáticos. No abarca el esfuerzo operativo razonable inherente a la aplicación de actualizaciones de programas informáticos o al mantenimiento de un entorno operativo seguro, como el tiempo del personal, las pruebas rutinarias, los ajustes de configuración o las actualizaciones de las dependencias de programas informáticos subyacentes que sean necesarios para gestionar componentes que hayan llegado al final de su vida útil o vulnerabilidades de seguridad conocidas. Por el contrario, los «costes adicionales» se refieren a cargas que van más allá de lo que cabe esperar normalmente en el contexto de las actualizaciones de los programas informáticos, como la adquisición obligatoria de nuevos equipos informáticos, la sustitución de infraestructuras o cambios fundamentales en el entorno operativo.

131. En el caso de los productos con elementos digitales consistentes en programas informáticos en constante evolución, los fabricantes pueden introducir en el mercado sucesivas versiones sustancialmente modificadas en intervalos relativamente cortos y esperar que los usuarios los actualicen periódicamente. En tales casos, el período de soporte declarado para cada versión sustancialmente modificada debe ajustarse a lo dispuesto en el artículo 13, apartado 8, en el momento de su comercialización. Es decir, el fabricante debe declarar un nuevo período de soporte para esa versión sustancialmente modificada. No obstante, los fabricantes podrán basarse en el artículo 13, apartado 10, para dejar de abordar y subsanar las vulnerabilidades de las versiones anteriores una vez que los usuarios puedan

actualizar a una versión posterior de forma gratuita y sin incurrir en los costes adicionales mencionados anteriormente, aunque ello dé lugar a un período de soporte efectivo más corto para dichas versiones anteriores ([18]). El fabricante sigue estando sujeto a los demás requisitos de gestión de las vulnerabilidades establecidos en la parte II del anexo I, así como a las obligaciones de información del artículo 14. Como también se explica en el considerando 40, estos requisitos incluyen, entre otras cosas, para todas las versiones posteriores sustancialmente modificadas del producto con elementos digitales consistente en un programa informático introducido en el mercado: i) disponer de una política de divulgación coordinada de vulnerabilidades; y ii) medidas para facilitar el intercambio de información sobre posibles vulnerabilidades ([19]).

Ejemplo 52: un fabricante introduce en el mercado de la UE un modelo de teléfono inteligente y declara un período de soporte de X años a partir de la fecha de introducción en el mercado, durante el cual proporcionará actualizaciones de seguridad para abordar las vulnerabilidades. Durante ese período, el fabricante publica periódicamente actualizaciones del programa informático y versiones sustancialmente modificadas del sistema operativo, que los usuarios pueden instalar de forma gratuita sin necesidad de nuevos equipos informáticos.

El fabricante podrá, de conformidad con el artículo 13, apartado 10, abordar y subsanar las vulnerabilidades de la versión más reciente del sistema operativo disponible para ese modelo de teléfono inteligente, siempre que las versiones anteriores puedan actualizarse de forma gratuita y sin costes adicionales. Durante el período de soporte, el fabricante sigue estando sujeto a los demás requisitos de gestión de las vulnerabilidades, como la divulgación coordinada de vulnerabilidades y las medidas de intercambio de información.

Ejemplo 53: un fabricante introduce en el mercado un producto empresarial con elementos digitales consistente en un programa informático y publica versiones sustancialmente modificadas cada pocos meses que incorporan mejoras de seguridad, nuevas funcionalidades y compatibilidad con sistemas operativos y plataformas actualizados. Cada versión se introduce en el mercado con un período de soporte declarado de conformidad con el artículo 13, apartado 8. El fabricante espera que los usuarios actualicen periódicamente el producto como parte del funcionamiento normal y proporciona acceso gratuito a la última versión. La aplicación de las actualizaciones puede requerir un esfuerzo operativo razonable, como ensayos o ajustes de configuración, pero no requiere costes adicionales, como la adquisición de equipos informáticos nuevos o cambios fundamentales en la infraestructura. En este contexto, el fabricante puede basarse en el artículo 13, apartado 10, para dejar de abordar y subsanar las vulnerabilidades de versiones anteriores una vez que los usuarios puedan actualizar el producto a la versión más reciente, sin dejar de cumplir los demás requisitos relativos a la gestión de vulnerabilidades para todas las versiones posteriores sustancialmente modificadas.

5.1. **Modificaciones sustanciales y período de soporte**

132. Como se establece en la sección 4.4 Consecuencias de una modificación sustancial, cuando una modificación de un producto con elementos digitales se considere una modificación sustancial y el producto con elementos digitales modificado se comercialice, debe tratarse como un producto nuevo a efectos del Reglamento de Ciberresiliencia, y el acto de comercializar el producto con elementos digitales sustancialmente modificado constituye una nueva introducción en el mercado. Por lo tanto, conviene aclarar las repercusiones que esta nueva introducción en el mercado tiene en el período de soporte del producto con elementos digitales sustancialmente modificado.

133. El período de soporte de un producto con elementos digitales sustancialmente modificado debe determinarse atendiendo al tiempo de utilización previsto de dicho producto, a la luz de los criterios establecidos en el artículo 13, apartado 8, del Reglamento de Ciberresiliencia. Por lo tanto, una modificación sustancial exige volver a evaluar el producto con arreglo a dichos criterios, pero no implica automáticamente que el período de soporte se restablezca ni siquiera que se amplíe. La cuestión pertinente es si la modificación sustancial afecta a los factores que determinaron originalmente el tiempo de utilización previsto de dicho producto y, por tanto, el período de soporte original.

([18]) Cabe recordar que el artículo 13, apartado 19, exige a los fabricantes, cuando sea técnicamente viable habida cuenta de la naturaleza del producto con elementos digitales, mostrar una notificación a los usuarios que les informe de que su producto con elementos digitales ha alcanzado el final de su período de soporte. Por lo tanto, cuando se dejen de abordar y subsanar las vulnerabilidades de versiones anteriores, se espera, siempre que sea técnicamente viable, que se informe a los usuarios que no hayan actualizado a la versión más reciente.

([19]) Cabe señalar que, cuando los usuarios puedan actualizar a la versión más reciente del programa informático sin costes adicionales, los fabricantes podrán, no obstante, optar por seguir abordando y subsanando las vulnerabilidades de versiones anteriores de dicho programa informático, incluso previo pago o mediante otras modalidades comerciales. El Reglamento de Ciberresiliencia no exige a los fabricantes que proporcionen actualizaciones de seguridad gratuitas para dichas versiones anteriores.

134. Cuando la modificación sustancial no afecte a dichos factores, los criterios establecidos en el artículo 13, apartado 8, seguirán indicando el mismo tiempo de utilización previsto que se determinó originalmente, y el período de soporte del producto con elementos digitales modificado deberá ajustarse al tiempo de utilización previsto restante del producto tal como se introdujo originalmente en el mercado. Este es generalmente el caso cuando el tiempo de utilización previsto se haya determinado principalmente en función de factores que la modificación no altera, como la durabilidad física de los componentes del equipo informático, afecta únicamente a las funcionalidades del programa informático o a los servicios de *back-end*.

Ejemplo 54: un fabricante introduce en el mercado un robot aspirador con un tiempo de utilización previsto de X años, determinado en función de la naturaleza del producto con elementos digitales, incluidas la durabilidad física y las características de desgaste de los componentes del equipo informático, y teniendo en cuenta las expectativas razonables de los usuarios en lo que respecta a la vida útil de dicho producto. El fabricante establece un período de soporte de X años. Al cabo de Y años, el fabricante publica una actualización del programa informático que constituye una modificación sustancial, y añade nuevos modos de limpieza y funcionalidades de navegación. La actualización del programa informático no afecta a la durabilidad física del equipo informático y no altera las expectativas razonables de los usuarios en lo que respecta a la vida útil del producto. Por lo tanto, los criterios del artículo 13, apartado 8, siguen indicando el mismo tiempo de utilización previsto. El período de soporte del producto con elementos digitales modificado se corresponde con el tiempo de utilización previsto restante determinado originalmente.

Ejemplo 55: un fabricante introduce en el mercado un producto con elementos digitales consistente en una maquinaria industrial compleja, con un servicio de back-end *en la nube que constituye una solución de tratamiento de datos a distancia. El tiempo de utilización previsto es de X años, determinado a la luz de las expectativas razonables de los usuarios y de la naturaleza del producto con elementos digitales, como la durabilidad física de la maquinaria y el desgaste previsto. El período de soporte se establece en consonancia con dicho tiempo de utilización previsto, en X años. Al cabo de Y años, el fabricante rediseña la arquitectura del servicio de* back-end *en la nube (la solución de tratamiento de datos a distancia), introduciendo nuevas API y flujos de datos, de una manera que constituye una modificación sustancial del producto con elementos digitales, pero que no altera la naturaleza de dicho producto ni afecta a las expectativas de los usuarios. Por lo tanto, los criterios del artículo 13, apartado 8, siguen indicando el mismo tiempo de utilización previsto. El período de soporte del producto con elementos digitales modificado se corresponde con el tiempo de utilización previsto restante determinado originalmente.*

135. Cuando la modificación sustancial afecte a los factores que determinaron inicialmente el tiempo de utilización previsto del producto con elementos digitales, el fabricante debe volver a calcular el período de soporte para reflejar el nuevo tiempo de utilización previsto, aplicando los criterios del artículo 13, apartado 8, en consecuencia. Este puede ser el caso, por ejemplo, de modificaciones de reacondicionamiento del equipo informático que amplíen la vida operativa de dicho producto, o de una reprogramación o reescritura sustancial del programa informático central del producto que modifique sustancialmente su tiempo de utilización previsto ([20]).

Ejemplo 56: un fabricante introduce en el mercado un controlador lógico programable con un tiempo de utilización previsto de X años, determinado principalmente en función de la naturaleza del producto con elementos digitales y la durabilidad del equipo informático subyacente. El período de soporte se establece en consecuencia. Varios años después de la introducción inicial en el mercado, el fabricante realiza una modificación sustancial consistente en sustituir la plataforma informática integrada del controlador lógico programable, que incluye el procesador, la memoria y el entorno de ejecución, por componentes de nueva generación diseñados para una vida útil operativa considerablemente más larga. Como consecuencia de la modificación, cambian las expectativas razonables de los usuarios y la naturaleza del producto con elementos digitales: ahora el usuario del controlador lógico programable puede esperar razonablemente que este siga en uso productivo más allá del tiempo de utilización previsto declarado inicialmente, gracias a la nueva plataforma informática. Por tanto, los criterios del artículo 13, apartado 8, indican un tiempo de utilización previsto más largo, y el fabricante vuelve a calcular en consecuencia el período de soporte para el controlador lógico programable en cuestión.

6. **PRODUCTOS IMPORTANTES Y CRÍTICOS CON ELEMENTOS DIGITALES**

136. El artículo 7, apartado 1, del Reglamento de Ciberresiliencia establece que los productos con elementos digitales cuya funcionalidad principal sea la de una categoría de productos establecida en el anexo III del Reglamento se considerarán «productos importantes con elementos digitales». El anexo III divide además los productos importantes con elementos digitales en las clases I y II. De igual modo, el artículo 8, apartado 1, establece que los productos con elementos digitales cuya funcionalidad principal sea la de una categoría de productos establecida en el anexo IV del Reglamento se considerarán «productos críticos con elementos digitales» ([21]).

([20]) Cabe recordar que, como se indica en la sección *4.1* Reparaciones físicas, las operaciones de reacondicionamiento, mantenimiento o reparación no se consideran, por lo general, modificaciones sustanciales.

([21]) El Reglamento de Ejecución (UE) 2025/2392 de la Comisión establece la descripción técnica de las categorías de productos importantes y críticos.

137. La clasificación de un producto con elementos digitales como importante o crítico o, por el contrario, como perteneciente a la categoría «por defecto» ([22]), es pertinente para determinar el procedimiento de evaluación de la conformidad que debe seguir el fabricante, con arreglo al artículo 32, antes de poder introducir dicho producto con elementos digitales en el mercado. En particular, los productos con elementos digitales incluidos de la categoría por defecto pueden acogerse siempre al procedimiento de control interno basado en el módulo A («autoevaluación») ([23]). Los productos importantes con elementos digitales de las clases I o II y los productos críticos con elementos digitales están sujetos a procedimientos de evaluación de la conformidad más estrictos. Esto no incluye los productos importantes con elementos digitales de las clases I o II que constituyen programas informáticos libres y de código abierto introducidos en el mercado, respecto de los cuales, de conformidad con el artículo 32, apartado 5, los fabricantes pueden seguir los procedimientos correspondientes a la categoría por defecto.

138. Por lo tanto, el concepto de funcionalidad principal es fundamental para que el fabricante determine el régimen de evaluación de la conformidad aplicable. Sin embargo, este concepto no está definido de forma explícita en el Reglamento de Ciberresiliencia. Los productos con elementos digitales pueden desempeñar una serie de funciones, algunas de las cuales pueden ser accesorias respecto de la funcionalidad principal de dicho producto, y no deben afectar a la clasificación del producto como «por defecto», «importante de clase I», «importante de clase II» o «crítico». Por tanto, conviene proporcionar más orientaciones para ayudar a los fabricantes a aplicar correctamente los procedimientos de evaluación de la conformidad pertinentes y ayudar a las autoridades de vigilancia del mercado a garantizar la aplicación armonizada del Reglamento de Ciberresiliencia en toda la UE.

6.1. **Funcionalidad principal**

139. La funcionalidad principal de un producto con elementos digitales hace referencia a sus principales características y capacidades técnicas, sin las cuales no podría cumplir su finalidad prevista. Esta puede evaluarse a la luz del contexto y las condiciones de utilización específicos del producto, teniendo en cuenta, entre otras cosas, la información que el fabricante proporciona en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, así como en la documentación técnica.

Ejemplo 57: un producto con elementos digitales consistente en un programa informático proporciona una capa de abstracción sobre el equipo informático subyacente y gestiona la ejecución de componentes de programas informáticos. Entre sus principales características figuran la inicialización del equipo informático y de los periféricos, la gestión de procesos y la memoria, el control de entradas y salidas, la planificación, la asignación de recursos y la exposición de servicios del sistema e interfaces de programación de aplicaciones (API) a través de las cuales las aplicaciones interactúan con los recursos de equipo informático y programas informáticos del dispositivo. La documentación técnica indica que el producto con elementos digitales orquesta los recursos informáticos, aplica las configuraciones del sistema y proporciona interfaces normalizadas para los módulos de programas informáticos y los periféricos conectados. El fabricante destaca que estas capacidades permiten a la plataforma servir de entorno central de programas informáticos en el que las aplicaciones pueden ejecutarse de forma fiable. El producto con elementos digitales tiene la funcionalidad principal de un sistema operativo, tal como se describe en el punto 11 del anexo I del Reglamento de Ejecución (UE) 2025/2392.

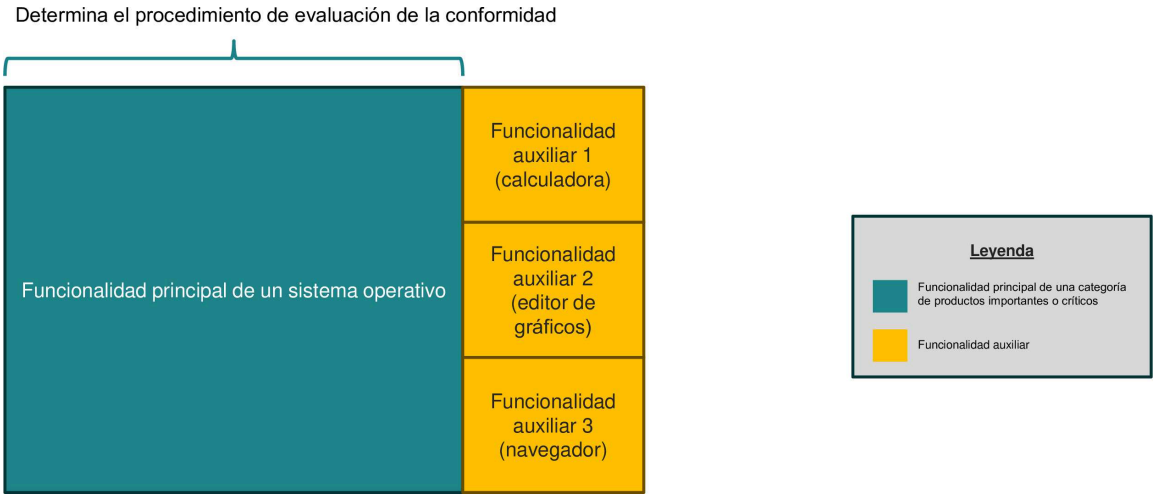
140. La funcionalidad de un producto con elementos digitales rara vez se limita exclusivamente a su funcionalidad principal, ya que los productos con elementos digitales a menudo, si no siempre, realizan funciones adicionales que no contribuyen a la funcionalidad principal del producto. Esto también puede incluir la incorporación de componentes que tengan la funcionalidad de otro producto importante o crítico con elementos digitales. Sin embargo, el hecho de que un producto con elementos digitales desempeñe funciones distintas o adicionales a las detalladas en las descripciones técnicas de productos importantes o críticos con elementos digitales no impide por sí mismo que el producto tenga una de esas funcionalidades principales.

([22]) El término «categoría por defecto» no es un término definido en el Reglamento de Ciberresiliencia. El uso de este término en el presente documento se refiere a productos con elementos digitales que no tienen la funcionalidad principal de una categoría de productos establecida en los anexos III o IV del Reglamento de Ciberresiliencia y que, por consiguiente, están sujetos al régimen de evaluación de la conformidad establecido en el artículo 32, apartado 1.

([23]) No obstante, el fabricante siempre puede optar por aplicar un procedimiento de evaluación de la conformidad más estricto, tal como se establece en el artículo 32, apartado 1.

Gráfico 2:

ilustración de cómo la funcionalidad principal, y no las funcionalidades auxiliares, determinan el procedimiento de evaluación de la conformidad aplicable



141. Un producto con elementos digitales puede tener la capacidad de desempeñar las funciones propias de una categoría de productos importantes o críticos y, a pesar de ello, tener una funcionalidad principal distinta de la correspondiente a dicha categoría de productos. En tales casos, dicho producto con elementos digitales no se consideraría un producto importante o crítico con elementos digitales. Como se establece expresamente en el artículo 7, apartado 1, del Reglamento de Ciberresiliencia con respecto a los productos importantes con elementos digitales (y aplicando la misma lógica, con respecto a los productos críticos con elementos digitales), la mera integración de un producto importante o crítico con elementos digitales no convierte por sí sola al producto en un producto importante o crítico con elementos digitales.

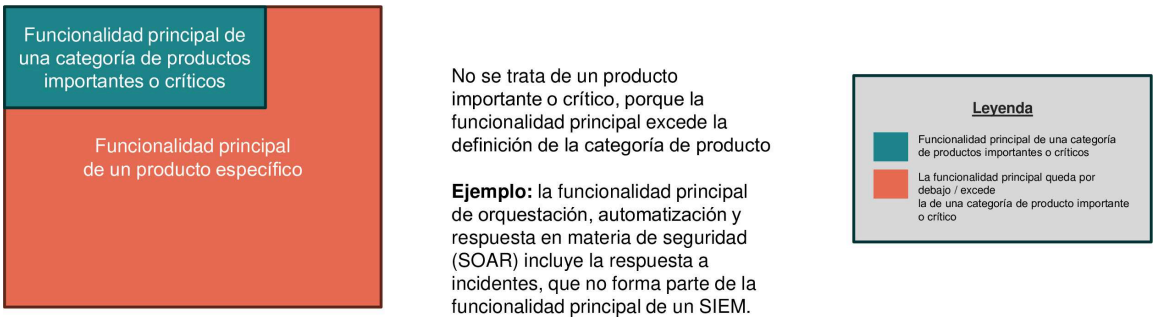
Ejemplo 58: un teléfono inteligente integra un sistema operativo que ofrece las funcionalidades descritas en el punto 11 del anexo I del Reglamento de Ejecución (UE) 2025/2392. Si bien el sistema operativo permite gestionar recursos de equipo informático y ejecutar aplicaciones de programas informáticos, el teléfono inteligente en su conjunto tiene una funcionalidad principal diferente (por ejemplo, permitir a los usuarios comunicarse y acceder a información y servicios). La mera integración de un sistema operativo no implica que el teléfono inteligente tenga la funcionalidad principal de un sistema operativo.

142. Algunos productos con elementos digitales pueden ser similares a una categoría de productos importantes o críticos, o pertenecer a la misma familia general de productos, pero su funcionalidad principal puede exceder sustancialmente o ser sustancialmente inferior a la funcionalidad principal de dicha categoría. No sucede así cuando un producto con elementos digitales incluye funcionalidades adicionales que simplemente complementan o mejoran la funcionalidad principal que de por sí corresponde a una categoría de productos importantes o críticos con elementos digitales; en tales casos, el producto con elementos digitales conserva la funcionalidad principal de dicha categoría y se clasifica en consecuencia. Esta evaluación debe basarse en las principales características y capacidades técnicas del producto, consideradas objetivamente a la luz de su finalidad prevista, y no en la forma en que se describa o comercialice el producto con elementos digitales cuando dicha descripción no refleje sus características técnicas reales.

Ejemplo 59: 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 de múltiples fuentes, analizarlos, correlacionarlos y presentarlos como información útil para fines relacionados con la seguridad. Sin embargo, la funcionalidad principal del programa informático supera sustancialmente la de un SIEM, pues incluye servicios como la respuesta a incidentes como elementos esenciales de sus capacidades técnicas. Por lo tanto, generalmente no se considera que el programa informático SOAR tenga la funcionalidad principal de los sistemas SIEM.

Gráfico 3:

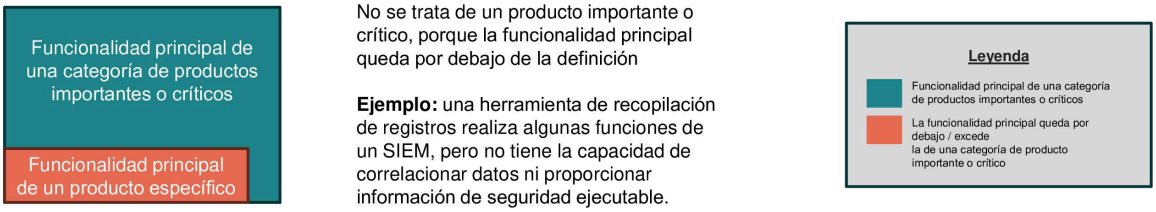
ilustración de la funcionalidad principal de un producto con elementos digitales que supera sustancialmente la definición de una categoría de productos importantes o críticos



Ejemplo 60: algunas herramientas de recopilación y visualización de registros tienen la capacidad de ingerir datos de registros y presentar cuadros de indicadores básicos que muestran eventos del sistema. Si bien estas herramientas pueden servir de apoyo a las actividades de supervisión de la seguridad, su funcionalidad principal es inferior a la de los sistemas SIEM, ya que no realizan correlación de datos ni proporcionan información útil sobre seguridad. Por lo tanto, generalmente no se considera que dichas herramientas tengan la funcionalidad principal de los sistemas SIEM.

Gráfico 4:

ilustración de la funcionalidad principal de un producto con elementos digitales que queda sustancialmente por debajo de la definición de una categoría de productos importantes o críticos

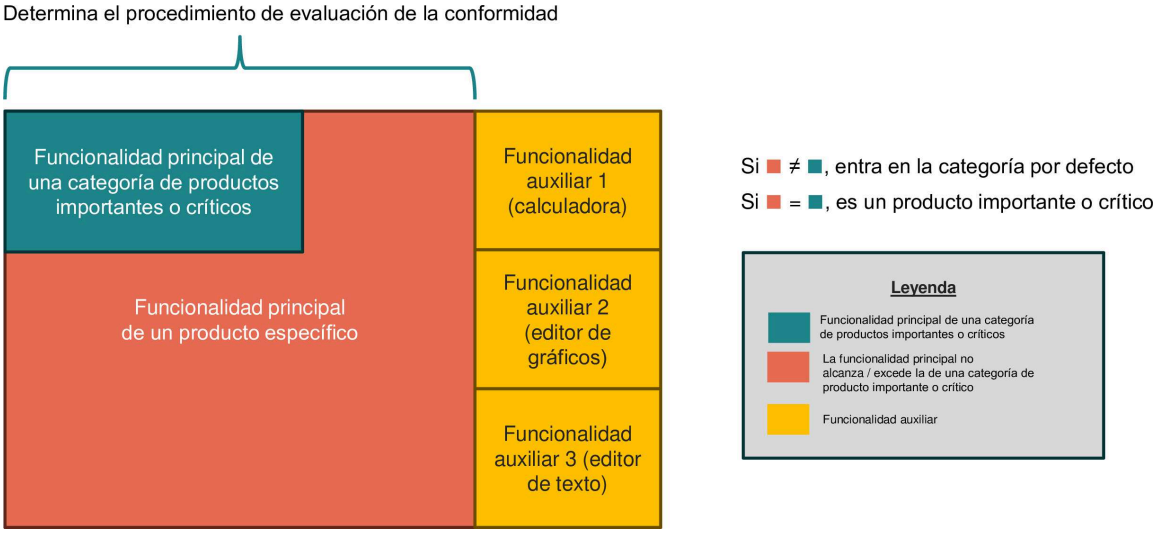


143. Un fabricante no puede presentar de forma engañosa la funcionalidad principal de su producto con elementos digitales con el fin de eludir el régimen de evaluación de la conformidad aplicable a los productos importantes o críticos con elementos digitales, por ejemplo, haciendo excesivo hincapié en determinadas funcionalidades o minimizando el papel de estas, de modo que el producto exceda sustancialmente una funcionalidad principal determinada o quede sustancialmente por debajo de ella. Este sería el caso, por ejemplo, cuando existan incoherencias manifiestas entre el material promocional, las instrucciones de uso y la documentación técnica.

144. A efectos de determinar el régimen de evaluación de la conformidad aplicable, un producto con elementos digitales no podrá tener más de una funcionalidad principal. De conformidad con el anexo VII del Reglamento de Ciberresiliencia, como parte de la documentación técnica de un producto, los fabricantes deben describir la finalidad prevista de su producto con elementos digitales y el procedimiento de evaluación de la conformidad que han seguido. Por lo tanto, la funcionalidad principal del producto debe estar claramente definida. Esto permite la correcta determinación del régimen de evaluación de la conformidad aplicable y permite a las autoridades de vigilancia del mercado supervisar y comprobar que el Reglamento se aplica correctamente.

Gráfico 5:

ilustración de cómo la funcionalidad principal de un producto con elementos digitales específico determina la clase de producto y, por tanto, el procedimiento de evaluación de la conformidad aplicable



145. Algunos productos con elementos digitales se introducen en el mercado como productos únicos con elementos digitales, pero están compuestos por módulos distintos con funcionalidades separadas. Cuando un fabricante también comercializa dichos módulos por separado, como en el caso de que se ofrezcan para su compra, concesión de licencia o suscripción por separado, dichos módulos constituyen por sí mismos productos con elementos digitales independientes. Como tales, deben clasificarse sobre la base de sus respectivas funcionalidades principales (y, por tanto, estarán sujetos al régimen de evaluación de la conformidad adecuado sobre la base de la funcionalidad principal de cada módulo). Esto se entiende sin perjuicio de los módulos que se suministren exclusivamente como componentes de un producto con elementos digitales integrado y que no estén disponibles por separado; en estos casos, la funcionalidad principal se determina a nivel del producto con elementos digitales integrado.

Ejemplo 61: un fabricante introduce en el mercado un conjunto unificado de soluciones de seguridad que combina varios módulos, entre ellos un SIEM, un sistema de detección de intrusiones y un módulo de análisis. El fabricante también ofrece estos módulos mediante suscripciones independientes. En este caso, cada módulo es un producto con elementos digitales distinto y se clasifica sobre la base de su propia funcionalidad principal. El módulo SIEM está sujeto al régimen de evaluación de la conformidad para productos importantes con elementos digitales de clase I, ya que su funcionalidad principal es la de los «sistemas de gestión de información y eventos de seguridad (SIEM)». El sistema de detección de intrusiones está sujeto al régimen de evaluación de la conformidad para productos importantes con elementos digitales de clase II, ya que su funcionalidad principal es la de «cortafuegos y sistemas de detección y prevención de intrusiones». El módulo de análisis está sujeto al régimen de evaluación de la conformidad para los productos «por defecto» con elementos digitales, ya que su funcionalidad principal no es la de una categoría de productos importantes ni críticos.

146. El incumplimiento de las obligaciones establecidas en el artículo 32 del Reglamento de Ciberresiliencia podrá dar lugar a multas administrativas de conformidad con el artículo 64, apartado 3.

6.2. Evaluación de la conformidad para productos importantes y críticos con elementos digitales

147. Una vez que el fabricante haya determinado la funcionalidad principal de su producto con elementos digitales, debe llevar a cabo uno de los procedimientos de evaluación de la conformidad aplicables. El fabricante debe garantizar que el producto con elementos digitales en su conjunto cumple los requisitos esenciales, teniendo en cuenta, según proceda, la seguridad de los componentes o funcionalidades integrados en él.

148. Es obligatorio un procedimiento de evaluación de la conformidad más estricto, con la participación de un tercero (basado en el módulo B+C, el módulo H o los esquemas de certificación de la ciberseguridad) para los productos importantes con elementos digitales de clase II (a excepción de los que constituyen programas informáticos libres y de código abierto, de conformidad con el artículo 32, apartado 5), así como para los productos críticos con elementos digitales ([24]). En cambio, los productos importantes con elementos digitales de clase I (a excepción de los que constituyen programas informáticos libres y de código abierto, de conformidad con el artículo 32, apartado 5) solo deben someterse a un procedimiento de evaluación de la conformidad por terceros si el fabricante no ha aplicado o ha aplicado solo parcialmente las normas armonizadas pertinentes cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* (en lo sucesivo, «normas armonizadas»), las especificaciones comunes o los esquemas europeos de certificación de la ciberseguridad con un nivel de garantía al menos «sustancial» ([25]).

149. Por lo tanto, para que un producto importante con elementos digitales de clase I pueda acogerse al procedimiento de control interno, i) deben aplicarse todos los requisitos aplicables de una norma armonizada pertinente; y ii) el ámbito de aplicación de la norma debe contemplar al menos todos los riesgos de ciberseguridad asociados a la funcionalidad principal de dicho producto.

150. la definición del producto con elementos digitales puede ser más amplia que la contemplada en la norma armonizada pertinente, y dichas funciones adicionales pueden presentar riesgos de ciberseguridad diferentes o adicionales. El fabricante siempre está obligado a llevar a cabo una evaluación de riesgos con arreglo al artículo 13, apartado 2, y, en consecuencia, debe comprobar si la aplicación de una norma armonizada abarca todos los riesgos asociados al producto con elementos digitales. Cuando la aplicación de la norma no abarque todos los riesgos, el fabricante debe garantizar por otros medios que su producto con elementos digitales cumple los requisitos esenciales.

151. Por lo tanto, si el fabricante de un producto importante con elementos digitales de clase I ha aplicado una norma armonizada pertinente que abarca los riesgos asociados a la funcionalidad principal del producto, puede decidir acogerse al procedimiento de control interno para demostrar la conformidad de su producto. Como parte de sus actividades de evaluación de la conformidad, el fabricante seguirá estando obligado a demostrar que se abordan todos los riesgos aplicables a su producto con elementos digitales. Por lo tanto, cuando exista una brecha entre la cobertura de la norma armonizada y la definición del producto con elementos digitales en su conjunto, el fabricante aún deberá igualmente documentar las medidas adicionales que haya adoptado para tratar dichos riesgos.

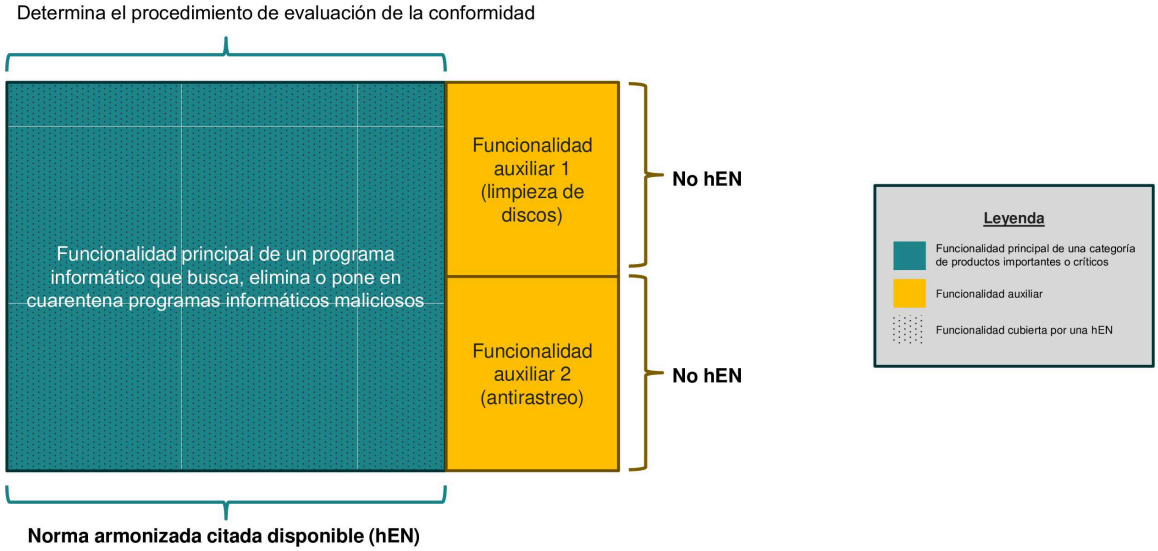
Ejemplo 62: un programa antivirus tiene la funcionalidad principal de un programa informático que busca, elimina o pone en cuarentena programas informáticos maliciosos, tal como se describe en el punto 4 del anexo I del Reglamento de Ejecución (UE) 2025/2392. Este producto con elementos digitales también incluye funcionalidades adicionales, a saber, una función de limpieza de discos y una función antirastreo que protege al usuario cuando navega por internet. El fabricante lleva a cabo una evaluación de riesgos que abarca el producto con elementos digitales en su totalidad, incluidas la funcionalidad principal del antivirus y las funciones de limpieza de discos y antirastreo. Aplica una norma armonizada que abarca los riesgos asociados a la funcionalidad principal del antivirus, así como medidas adicionales para hacer frente a los riesgos derivados de funciones adicionales. El fabricante puede acogerse al procedimiento de control interno para su evaluación de la conformidad, que abarca la totalidad del producto con elementos digitales, incluidas las funciones de limpieza de discos y antirastreo.

([24]) Este es también el caso cuando se utiliza un régimen europeo de certificación de la ciberseguridad con un nivel de garantía al menos «sustancial», ya que se requiere la participación de un organismo de certificación tercero.

([25]) En aras de la brevedad, el resto de la presente sección solo se refiere a las normas armonizadas cuyas referencias se han publicado en el *Diario Oficial de la Unión Europea*. No obstante, las mismas orientaciones también se aplican a las especificaciones comunes adoptadas de conformidad con el artículo 27, apartado 2, y a los esquemas europeos de certificación de la ciberseguridad cuando así lo especifique la Comisión mediante actos delegados de conformidad con el artículo 27, apartado 9.

Gráfico 6:

ilustración de cómo el uso de una norma armonizada citada que cubre únicamente la funcionalidad principal determina el procedimiento de evaluación de la conformidad aplicable



152. Este es también el caso cuando el producto con elementos digitales integra una función adicional que es, a su vez, la de otro producto importante o crítico con elementos digitales. De hecho, es la funcionalidad principal del producto con elementos digitales en su conjunto, y no la funcionalidad de los componentes integrados considerados de forma aislada, la que determina si el producto con elementos digitales pertenece a la categoría de productos importantes o críticos (y, por tanto, el régimen de evaluación de la conformidad aplicable). Por ejemplo, si un producto con elementos digitales tiene la funcionalidad principal de un producto importante con elementos digitales de clase I, dicho producto en su conjunto está sujeto al régimen de evaluación de la conformidad aplicable a los productos importantes con elementos digitales de clase I, aunque integre un componente que sea, por sí mismo, un producto crítico con elementos digitales. En estos casos, cuando el fabricante aplique una norma armonizada que contemple los riesgos asociados a la funcionalidad principal de dicho producto, puede acogerse al procedimiento de control interno.

Ejemplo 63: un producto con elementos digitales consistente en un equipo informático tiene la funcionalidad principal de un enrutador, tal como se describe en el punto 12 del anexo I del Reglamento de Ejecución (UE) 2025/2392. Dicho producto con elementos digitales también incluye funcionalidades adicionales, entre ellas funcionalidades de cortafuegos, ya que integra un componente de cortafuegos. El fabricante lleva a cabo una evaluación de riesgos que abarca el producto con elementos digitales en su totalidad, entre ellas la funcionalidad principal del enrutador y la funcionalidad de cortafuegos. Aplica una norma armonizada que abarca los riesgos asociados a la funcionalidad principal del enrutador, así como medidas adicionales para hacer frente a los riesgos derivados de funciones adicionales. Por ejemplo, el fabricante puede aplicar la norma armonizada para los cortafuegos a fin de cubrir los riesgos asociados a la funcionalidad de cortafuegos. El fabricante puede acogerse al procedimiento de control interno para su evaluación de la conformidad, que abarca la totalidad del producto con elementos digitales, incluida la funcionalidad de cortafuegos.

6.3. Implicaciones para la presunción de conformidad

153. El artículo 27, apartado 1, del Reglamento de Ciberresiliencia establece que «[s]e presumirá que los productos con elementos digitales y los procesos establecidos por el fabricante que sean conformes con normas armonizadas o partes de estas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* (DOUE), son conformes con los requisitos esenciales de ciberseguridad establecidos en el anexo I que estén regulados por dichas

normas o partes de ellas» ([26]). El artículo 27, apartado 5, amplía la misma presunción de conformidad a los productos con elementos digitales y a los procesos establecidos por el fabricante que sean conformes con las especificaciones comunes adoptadas por la Comisión mediante actos de ejecución, y el artículo 27, apartado 8, establece la presunción de conformidad de los productos con elementos digitales y los procesos establecidos por el fabricante para los que se haya expedido una declaración UE de conformidad o un certificado en el marco de un esquema europeo de certificación de la ciberseguridad adoptado en virtud del Reglamento (UE) 2019/881, si esto se ha especificado mediante actos delegados de conformidad con el artículo 27, apartado 9 ([27]).

154. Por lo tanto, cuando el fabricante haya aplicado una norma armonizada cuyas referencias se hayan publicado en el DOUE, se beneficiará de una presunción de conformidad respecto de los riesgos cubiertos por dicha norma. Este podría ser el caso, por ejemplo, cuando la norma armonizada referenciada abarque todos los riesgos asociados a la funcionalidad principal de un producto con elementos digitales y no existan funcionalidades adicionales que presenten riesgos de ciberseguridad. Por ejemplo, cabe esperar que la norma armonizada aplicable a los enrutadores abarque, como mínimo, los riesgos asociados a la funcionalidad principal de estos productos con elementos digitales. Si dicho producto no contiene ninguna funcionalidad adicional o si dichas funcionalidades adicionales no presentan riesgos que no estén cubiertos por la norma, el producto con elementos digitales puede beneficiarse de una presunción de conformidad.

155. En los casos analizados en los puntos 151 y 152, el fabricante puede utilizar el procedimiento de control interno porque la norma armonizada abarca los riesgos asociados a la funcionalidad principal del producto con elementos digitales. Sin embargo, los productos con elementos digitales descritos en dichos ejemplos pueden tener una definición más amplia que las normas armonizadas, y las funcionalidades adicionales pueden presentar riesgos de ciberseguridad que no estén contemplados en dichas normas armonizadas. Por lo tanto, esos productos con elementos digitales pueden no beneficiarse de una presunción de conformidad respecto de dichas funcionalidades adicionales.

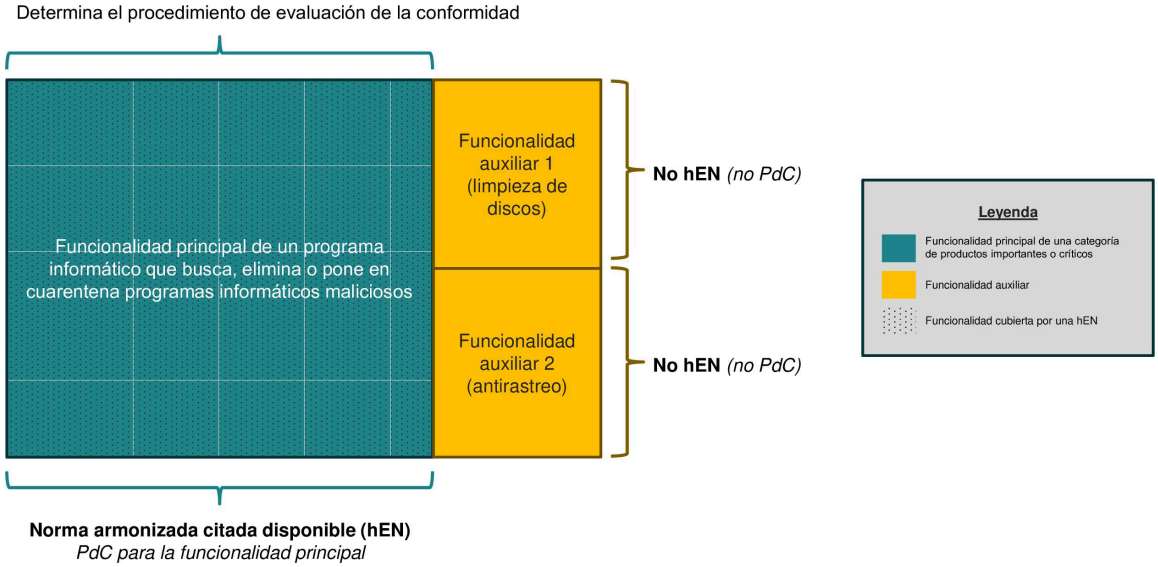
Ejemplo 64: un programa antivirus tiene la funcionalidad principal de un programa informático que busca, elimina o pone en cuarentena programas informáticos maliciosos, y los riesgos asociados a dicha funcionalidad principal están cubiertos por la norma armonizada. Este producto con elementos digitales también incluye funcionalidades adicionales, a saber, una función de limpieza de discos y una funcionalidad antirastreo que protege al usuario cuando navega por internet. Los riesgos de estas funcionalidades adicionales no están cubiertos por la norma armonizada. Si se aplica la norma armonizada, el fabricante puede acogerse al procedimiento de control interno para su evaluación de la conformidad. Se beneficiará de una presunción de conformidad respecto de los riesgos asociados a la funcionalidad principal de dicho producto, pero no respecto de los riesgos asociados a las funcionalidades adicionales.

([26]) Como se indica claramente en la sección 4.1.2.2 de la Guía azul, «[e]n el caso de la legislación de armonización relacionada con los riesgos, [...] un fabricante siempre, incluso cuando emplee normas armonizadas cuyas referencias se publiquen en el *Diario Oficial de la Unión Europea*, es plenamente responsable de la evaluación de todos los riesgos de su producto para determinar qué requisitos esenciales (o de otro tipo) son pertinentes. Tras esta evaluación, el fabricante puede optar por aplicar las especificaciones técnicas incluidas en las normas armonizadas cuyas referencias se publiquen en el *Diario Oficial de la Unión Europea* para introducir las "medidas de reducción del riesgo" especificadas por las normas armonizadas».

([27]) Como se ha indicado, en aras de la brevedad, el resto de la presente sección solo se refiere a las normas armonizadas cuyas referencias se han publicado en el *Diario Oficial de la Unión Europea*. Sin embargo, las mismas orientaciones también se aplican a las especificaciones comunes y a los esquemas europeos de certificación de la ciberseguridad.

Gráfico 7:

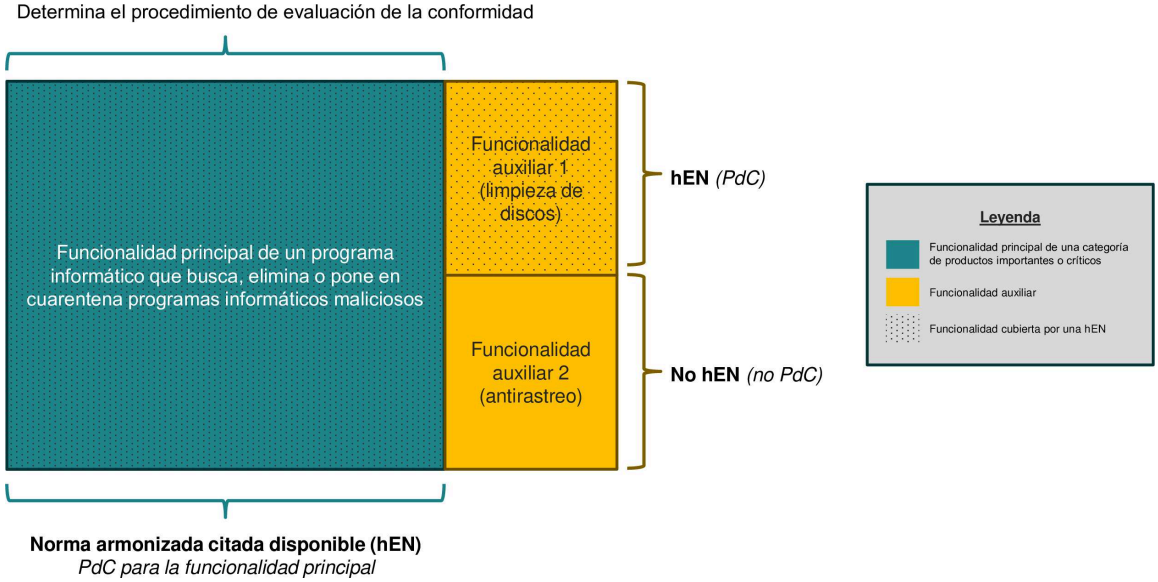
la norma armonizada otorga la presunción de conformidad respecto de la funcionalidad principal, ya que aborda todos los riesgos asociados a dicha funcionalidad, pero no respecto de las funcionalidades adicionales



Ejemplo 65: en el mismo escenario que el ejemplo anterior, la norma armonizada se ha actualizado para abarcar también los riesgos asociados a una de las funcionalidades adicionales, a saber, la función de limpieza de discos, pero no la otra (esto decir, la función antirastreo). Si se aplica la norma armonizada, el fabricante puede acogerse al procedimiento de control interno para su evaluación de la conformidad. Se beneficiará de una presunción de conformidad respecto de los riesgos asociados a la funcionalidad principal de dicho producto y a la funcionalidad de limpieza de discos, pero no respecto de los riesgos asociados a la funcionalidad antirastreo.

Gráfico 8:

la norma armonizada otorga la presunción de conformidad respecto de la funcionalidad principal y la funcionalidad auxiliar 1, ya que aborda todos los riesgos asociados a esas dos funcionalidades, pero no respecto de la funcionalidad auxiliar 2



7. **EVALUACIÓN DE LOS RIESGOS DE CIBERSEGURIDAD E INTEGRACIÓN DE PRODUCTOS CON ELEMENTOS Y COMPONENTES DIGITALES**

7.1. **Sobre la evaluación y el tratamiento de los riesgos de ciberseguridad**

156. La evaluación de los riesgos de ciberseguridad prevista en el artículo 13, apartado 2, del Reglamento de Ciberresiliencia exige a los fabricantes que determinen los riesgos pertinentes y evalúen sus posibles repercusiones en el producto con elementos digitales. Los fabricantes también deben aplicar las medidas adecuadas para hacer frente a estos riesgos, de conformidad con los requisitos esenciales del anexo I.

157. En la gestión de riesgos organizativos, los riesgos suelen evaluarse con arreglo a criterios de aceptación derivados de los objetivos internos de la organización o de su apetito de riesgo. En cambio, en el marco del Reglamento de Ciberresiliencia, el riesgo de ciberseguridad residual debe evaluarse a la luz del requisito de que el producto con elementos digitales introducido en el mercado garantice un nivel adecuado de ciberseguridad basado en los riesgos, teniendo en cuenta su finalidad prevista y su uso razonablemente previsible.

158. Por consiguiente, la tolerancia interna al riesgo del fabricante, su estrategia comercial o las meras consideraciones de costes no son pertinentes para determinar si se han abordado los riesgos. A efectos del artículo 13, apartados 2 y 3, los fabricantes deben estar en condiciones de determinar si los riesgos de ciberseguridad detectados se han abordado de manera suficiente mediante la aplicación de los requisitos esenciales de la parte I del anexo I, a la luz de la finalidad prevista, el uso razonablemente previsible y las condiciones de utilización, incluido, cuando corresponda, el entorno operativo (por ejemplo, los usuarios previstos del producto con elementos digitales) y los activos que deben protegerse, teniendo en cuenta el tiempo durante el cual se prevé que el producto con elementos digitales esté en uso.

159. El riesgo de ciberseguridad residual es un resultado inherente de la evaluación y el tratamiento de riesgos. Se reconoce que, en la práctica, los riesgos de ciberseguridad no pueden eliminarse por completo. No obstante, la existencia de un riesgo residual no implica que el fabricante pueda aceptar cualquier riesgo a su discreción. Un producto con elementos digitales solo podrá introducirse en el mercado cuando los riesgos residuales, una vez adoptadas las medidas adecuadas, se hayan abordado de manera suficiente mediante la aplicación de los requisitos esenciales, teniendo en cuenta la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales.

160. De conformidad con el artículo 13, apartado 3, cuando se detecten riesgos de ciberseguridad, los fabricantes deben abordarlos mediante medidas adecuadas, también a nivel del producto. Dependiendo de las circunstancias, esto puede implicar, por ejemplo, reducir la superficie de ataque, aplicar medidas técnicas de protección, limitar o adaptar la funcionalidad o definir con mayor precisión la finalidad prevista del producto con elementos digitales. Los fabricantes también pueden adoptar medidas para configurar el uso razonablemente previsible del producto con elementos digitales, por ejemplo, comunicando los riesgos, ofreciendo orientaciones al usuario o diseñando interfaces de usuario, con el fin de orientar el comportamiento del usuario hacia pautas de uso seguras.

161. El Reglamento de Ciberresiliencia no contempla la transferencia del riesgo o la responsabilidad en materia de ciberseguridad a los usuarios o a terceros para compensar deficiencias en el diseño del producto o justificar que no se aborden los riesgos de ciberseguridad. La obligación de introducir en el mercado un producto con elementos digitales seguro y de demostrar la conformidad con los requisitos esenciales sigue siendo exclusivamente del fabricante.

162. La información y las instrucciones proporcionadas a los usuarios pueden utilizarse para facilitar la implantación y el funcionamiento seguros del producto con elementos digitales, también cuando el fabricante haya optado por restringir la finalidad prevista de dicho producto a entornos de confianza, y para informar a los usuarios de los riesgos residuales, de manera adecuada a la naturaleza del producto con elementos digitales y a sus usuarios previstos.

Ejemplo 66: un fabricante desarrolla un sensor industrial destinado a utilizarse en entornos de confianza. Para que el sensor pueda desempeñar correctamente su funcionalidad, el fabricante no aplica medidas de protección contra ataques físicos dirigidos al propio sensor. A fin de mitigar los riesgos asociados detectados en la evaluación de riesgos, el fabricante limita la finalidad prevista del sensor a su utilización únicamente en entornos de confianza en los que se impida el acceso físico no autorizado al producto con elementos digitales. La información y las instrucciones a los usuarios proporcionan información clara sobre estas limitaciones de utilización del sensor, de manera adecuada a la naturaleza del producto con elementos digitales y a sus usuarios previstos.

Ejemplo 67: un fabricante desarrolla una aplicación de programa informático destinada a un uso profesional en dispositivos de mesa y móviles gestionados. La aplicación procesa datos sensibles almacenados localmente y contenidos generados por los usuarios. Durante la evaluación del riesgo, el fabricante detecta el riesgo de acceso no autorizado a dichos datos si se almacenan en texto claro en el dispositivo. En lugar de diseñar y aplicar un mecanismo de cifrado propio dentro de la aplicación, el fabricante opta por basarse en las funciones de cifrado y gestión de claves proporcionadas de forma nativa por el sistema operativo en el que está previsto que se ejecute la aplicación, ya que los servicios criptográficos integrados en el sistema operativo están maduros y reciben mantenimiento periódico.

163. Cuando la evaluación de los riesgos de ciberseguridad detecte riesgos que no puedan abordarse de forma adecuada mediante medidas apropiadas, el cumplimiento del Reglamento de Ciberresiliencia puede requerir modificaciones en el diseño, la funcionalidad o la finalidad prevista del producto con elementos digitales. Las consideraciones relativas únicamente al coste o la viabilidad comercial no constituyen motivos suficientes para no abordar dichos riesgos cuando ello impida que el producto con elementos digitales cumpla los requisitos esenciales.

7.2. Sobre el diseño, el desarrollo y la producción de productos con elementos digitales de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes

164. El requisito esencial de ciberseguridad a que se refiere el punto 1 de la parte I del anexo I del Reglamento de Ciberresiliencia establece que los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes.

165. Este requisito esencial tiene por objeto abordar todos los riesgos de ciberseguridad que se hayan detectado como parte de la evaluación de los riesgos de ciberseguridad. En particular, esto incluye los riesgos de ciberseguridad que no se abordan adecuadamente de otro modo como parte de la aplicación de los requisitos esenciales de la parte I del anexo I, distintos del punto 1. Este requisito esencial es diferente de la obligación jurídica de llevar a cabo una evaluación de los riesgos de ciberseguridad, que debe realizarse de conformidad con el artículo 13, apartado 2.

166. Cuando todos los riesgos de ciberseguridad pertinentes relacionados con un producto con elementos digitales se aborden mediante la aplicación de medidas adecuadas para abordar los requisitos esenciales aplicables distintos del punto 1, se considerará que se cumple el requisito esencial a que se refiere el punto 1 de la parte I del anexo I. Por el contrario, cuando la evaluación de los riesgos de ciberseguridad determine que existen riesgos adicionales que no se abordan plenamente mediante dichas medidas, los fabricantes están obligados a aplicar medidas adecuadas en el producto con elementos digitales para abordar dichos riesgos, de modo que cumplan el requisito esencial a que se refiere el punto 1 de la parte I del anexo I. En la práctica, en la mayoría de los casos, se espera que el cumplimiento de los demás requisitos esenciales dé lugar al cumplimiento de este requisito.

7.3. Evaluación de riesgos y diligencia debida en relación con las dependencias externas y los componentes integrados

167. El Reglamento de Ciberresiliencia establece dos obligaciones distintas, aunque complementarias, para los fabricantes en relación con la gestión de los riesgos de ciberseguridad. En primer lugar, el artículo 13, apartado 2, exige a los fabricantes que lleven a cabo una evaluación de los riesgos de ciberseguridad del propio producto con elementos digitales. En segundo lugar, el artículo 13, apartado 5, impone la obligación de ejercer la diligencia debida con respecto a los componentes integrados. En conjunto, estas dos obligaciones están diseñadas para garantizar que el producto con elementos digitales siga siendo seguro, aun cuando se base en soluciones de tratamiento de datos a distancia, servicios a distancia o componentes de equipos o programas informáticos de terceros.

168. La evaluación de los riesgos de ciberseguridad se refiere a la detección y gestión de los riesgos pertinentes que puedan afectar al producto con elementos digitales, incluidos los riesgos que se originan fuera del propio producto, como las redes externas, los factores ambientales u otros aspectos externos que puedan afectar al producto con elementos digitales o de los que este dependa. En lo que respecta a estos riesgos externos, el Reglamento de Ciberresiliencia no exige a los fabricantes controlar ni gestionar el entorno externo. Por el contrario, los fabricantes están obligados a determinar dichos riesgos y a mitigarlos mediante el diseño y el desarrollo del producto con elementos digitales. Esto implicará aplicar los requisitos esenciales adecuados establecidos en la parte I del anexo I y, en caso necesario, proporcionar información e instrucciones a los usuarios sobre los riesgos relacionados con la integración o la implantación.

169. Por ejemplo, un fabricante puede detectar el riesgo de que personas no autorizadas obtengan acceso a sistemas *back-end* que no formen parte del propio producto con elementos digitales mientras este se encuentra en funcionamiento, y que intenten enviar comandos maliciosos al producto con elementos digitales. Estos sistemas *back-end*, cuando no los ha diseñado ni desarrollado el fabricante, o bajo su responsabilidad, o cuando no sean compatibles con una de las funciones del producto con elementos digitales, no constituyen soluciones de tratamiento de datos a distancia y, por tanto, quedan fuera del ámbito de aplicación del producto con elementos digitales a efectos del Reglamento de Ciberresiliencia. No obstante, el Reglamento de Ciberresiliencia exige al fabricante que aborde el riesgo que dichos sistemas pueden plantear mediante medidas a nivel del producto, como exigir la autenticación criptográfica de los comandos remotos, verificar la integridad de los cambios de configuración o generar registros o alertas pertinentes para la seguridad cuando se detecte un comportamiento anómalo. Del mismo modo, cuando un fabricante detecte un riesgo derivado de la indisponibilidad de dicho servicio externo, por ejemplo, debido a interrupciones del suministro eléctrico o fallos de la infraestructura, el Reglamento de Ciberresiliencia puede exigir medidas de mitigación a nivel del producto contra tales riesgos de ciberseguridad, como garantizar que la interrupción del servicio no haga que el producto con elementos digitales pase a un estado que no sea seguro. En estos casos, el Reglamento de Ciberresiliencia regula la forma en que el producto con elementos digitales responde a dichos riesgos externos; no impone obligaciones sobre cómo se organiza, se dota de personal o se explota la infraestructura de *back-end*, ni considera dicha infraestructura parte del producto con elementos digitales.

170. La diligencia debida se refiere a los elementos que forman parte del propio producto con elementos digitales, en particular a los componentes de programas o de equipos informáticos integrados proporcionados por un tercero. Los fabricantes están obligados a adoptar las medidas adecuadas para garantizar que dichos componentes no socaven la conformidad del producto con elementos digitales con los requisitos esenciales. Esto solo puede lograrse determinando lo que el producto con elementos digitales requiere de sus componentes para cumplir sus objetivos de ciberseguridad y verificando, con un enfoque basado en los riesgos, que dichos componentes respondan a las necesidades del producto, como también se indica en el considerando 34.

171. En consonancia con su evaluación de los riesgos de ciberseguridad, el fabricante debe determinar los requisitos que debe cumplir el componente integrado. Por ejemplo, si el producto con elementos digitales se basa en funciones criptográficas, mecanismos de actualización o comunicaciones seguras proporcionados por un componente, el fabricante debe, como parte de su diligencia debida, determinar dichas necesidades y verificar que el componente las satisface. Las pruebas a tal efecto pueden consistir en documentación obtenida del fabricante del componente, como especificaciones técnicas, documentación de seguridad o documentación pertinente sobre la conformidad o el nivel de garantía. Cuando corresponda, el fabricante también podrá realizar pruebas para verificar que dichos componentes cumplen debidamente las funciones pertinentes. Si bien la diligencia debida constituye una obligación jurídica independiente, sirve para respaldar y sustentar la capacidad del fabricante para demostrar la conformidad con los requisitos esenciales del producto con elementos digitales en su conjunto.

172. Al evaluar los riesgos para el producto con elementos digitales en su conjunto, los elementos ajenos al producto, como los elementos ambientales, la infraestructura externa y otros sistemas o redes, deben tenerse en cuenta en la evaluación de los riesgos de ciberseguridad y, cuando proceda, abordarse mediante medidas a nivel del producto para garantizar la conformidad del producto con elementos digitales con los requisitos esenciales. Los componentes que estén física o lógicamente integrados en el producto con elementos digitales, pero que procedan de un tercero, también deben considerarse parte de la evaluación de riesgos. No obstante, a efectos de cumplimiento, el fabricante debe tratarlos como componentes suministrados externamente cuyas propiedades se verifican mediante la diligencia debida en el momento de su integración, ya que es posible que el fabricante no los haya rediseñado ni desarrollado de nuevo.

173. La misma lógica se aplica durante el desarrollo y la integración de los componentes. Cuando el propio fabricante desarrolle funcionalidades, debe aplicar directamente los requisitos esenciales. Cuando el fabricante integre componentes desarrollados por terceros, debe garantizar, mediante la diligencia debida, que dichos componentes puedan utilizarse de manera que el producto con elementos digitales en su conjunto cumpla los requisitos aplicables. En ambos casos, el objetivo sigue siendo el mismo: que el producto con elementos digitales, tal como se introduce en el mercado, alcance un nivel adecuado de ciberseguridad, tal como exige el Reglamento de Ciberresiliencia, teniendo en cuenta los riesgos detectados en la evaluación de los riesgos de ciberseguridad.

7.4. **Reutilización de las evaluaciones de riesgos y la documentación de conformidad para familias de productos con elementos digitales**

174. Los fabricantes pueden introducir en el mercado productos con elementos digitales que sean similares, por ejemplo, distintas variantes, modelos o configuraciones de la misma familia de productos. Cuando dichos productos con elementos digitales comparten la misma arquitectura, el mismo diseño en lo referente a la seguridad y la misma finalidad prevista, y están expuestos a los mismos riesgos de ciberseguridad, el Reglamento de Ciberresiliencia no exige a los fabricantes que traten cada variante como un producto con elementos digitales completamente independiente a efectos de la evaluación de riesgos y la evaluación de la conformidad.

175. En tales casos, siempre que todas las variantes en cuestión estén adecuadamente cubiertas en cuanto a los riesgos pertinentes y los requisitos esenciales, los fabricantes pueden basarse en: i) una única evaluación de los riesgos de ciberseguridad realizada de conformidad con el artículo 13, apartado 2, del Reglamento de Ciberresiliencia; ii) un único conjunto de documentación técnica; y iii) un único procedimiento de evaluación de la conformidad. Esto también permite emitir una única declaración UE de conformidad para el grupo de productos con elementos digitales, siempre que identifique claramente las variantes de productos a las que se aplica.

176. El factor determinante es si las diferencias entre las variantes son pertinentes desde el punto de vista de la ciberseguridad. Las variaciones que no afectan a las propiedades de ciberseguridad del producto con elementos digitales, como las diferencias de color, factor de forma, tamaño de la memoria u otras características no pertinentes para la seguridad, no requieren evaluaciones de riesgos ni evaluaciones de la conformidad independientes. Por el contrario, en algunos casos las variantes pueden diferir en formas que afecten a la aplicación de los requisitos esenciales, por ejemplo, debido a diferencias en las interfaces de comunicación, las pilas de los programas informáticos, los mecanismos de actualización o la conectividad remota. En tales casos, esas diferencias deben reflejarse en la evaluación de riesgos y, en caso necesario, en la evaluación de la conformidad y en la documentación técnica.

177. Los fabricantes siguen siendo responsables de garantizar que la evaluación de riesgos y la documentación correspondiente reflejen con exactitud los productos con elementos digitales introducidos en el mercado. Cuando una nueva variante introduzca nuevos riesgos de ciberseguridad o modifique la forma en que se aplican los requisitos esenciales, la evaluación de riesgos y la documentación relativa a la evaluación de la conformidad existentes deben actualizarse en consecuencia. Solo es posible basarse en una única evaluación de la conformidad en la medida en que los productos con elementos digitales no presenten diferencias en cuanto a sus propiedades de ciberseguridad.

8. **TRATAMIENTO DE DATOS A DISTANCIA**

178. El artículo 3, punto 1, del Reglamento de Ciberresiliencia define un producto con elementos digitales como un «producto consistente en programas informáticos o equipos informáticos y sus soluciones de tratamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado». En este sentido, el fabricante debe considerar el producto con elementos digitales en su conjunto, incluidas sus soluciones de tratamiento de datos a distancia. Por ejemplo, al demostrar que el producto con elementos digitales cumple los requisitos esenciales establecidos en el anexo I, deben tenerse en cuenta las soluciones de tratamiento de datos a distancia, empezando por la evaluación de riesgos (artículo 13, apartado 2). Lo mismo se aplica al considerar las obligaciones relativas al ciclo de vida, como la notificación de vulnerabilidades aprovechadas activamente y de incidentes graves (artículo 14).

179. El objetivo de las presentes orientaciones es prestar más apoyo a los fabricantes a la hora de determinar si su producto con elementos digitales tiene soluciones de tratamiento de datos a distancia, tal como se definen en el Reglamento de Ciberresiliencia, y cómo cumplir sus obligaciones de conformidad correspondientes a este respecto. Tras un análisis inicial de las definiciones y los considerandos establecidos en el Reglamento de Ciberresiliencia, las presentes orientaciones formularán preguntas destinadas a orientar a los fabricantes a la hora de aclarar si su producto con elementos digitales incluye o no soluciones de tratamiento de datos a distancia (véase la sección *8.1* ¿Qué se considera una solución de tratamiento de datos a distancia para un producto con elementos digitales?). Posteriormente, profundizará en las implicaciones técnicas de las soluciones de tratamiento de datos a distancia y en cómo evaluar la conformidad con el Reglamento de Ciberresiliencia (véase la sección *8.2* Implicaciones prácticas y técnicas de las soluciones de tratamiento de datos a distancia y dependencia de soluciones de terceros).

180. El artículo 3, punto 2, define el concepto de «tratamiento de datos a distancia» como el «tratamiento de datos a distancia para el que el programa informático ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad y cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones». Por lo tanto, las soluciones de tratamiento de datos a distancia se definen como los elementos de programa informático («la parte de un sistema electrónico de información consistente en un código informático», tal como se define en el artículo 3, punto 4) del tratamiento de datos a distancia. No se pretende que formen parte del ámbito de aplicación del producto con elementos digitales los equipos informáticos en los que pueda basarse el tratamiento de datos a distancia.

181. Los considerandos 11 y 12 ofrecen más explicaciones sobre cómo debe interpretarse este concepto. El considerando 11 aclara que el objetivo de incluir las soluciones de tratamiento de datos a distancia es que los «productos estén adecuadamente protegidos en su totalidad por sus fabricantes, con independencia de que los datos sean tratados o almacenados localmente en el dispositivo del usuario o a distancia por el fabricante». Asimismo, establece que «[l]os requisitos relativos a las soluciones de tratamiento de datos a distancia que entran en el ámbito de aplicación del presente Reglamento no implican, por tanto, medidas técnicas, operativas u organizativas destinadas a gestionar los riesgos para la seguridad de las redes y los sistemas de información de un fabricante en su conjunto».

182. Por lo tanto, del considerando 11 se desprende que la intención no es que los requisitos del Reglamento de Ciberresiliencia se apliquen a toda la infraestructura informática de una organización, sino únicamente a los componentes de programas informáticos que permitan ejecutar la solución de tratamiento de datos. Por ejemplo, los sistemas internos relacionados con los recursos humanos propios del fabricante, las nóminas, la gestión de las relaciones con los clientes, los procesos de integración/entrega continua y la distribución de actualizaciones de seguridad a ubicaciones periféricas no deben considerarse soluciones de tratamiento de datos a distancia. Del mismo modo, los sistemas relacionados con las actividades de auditoría y realización de pruebas, como las pruebas de penetración, la búsqueda de amenazas y la utilización de «equipos rojos», quedan fuera del ámbito de aplicación de un producto con elementos digitales a efectos del Reglamento de Ciberresiliencia. Es importante señalar que, si bien la realización de pruebas y revisiones eficaces y periódicas de la seguridad del producto con elementos digitales constituye un requisito esencial establecido en el punto 3 de la parte II del anexo I del Reglamento de Ciberresiliencia, esto no significa que dichas actividades deban considerarse soluciones de tratamiento de datos a distancia del producto con elementos digitales.

183. El considerando 12 se centra en los servicios en la nube y detalla las circunstancias en las que los servicios en la nube podrían considerarse soluciones de tratamiento de datos a distancia. El considerando concluye recordando que los servicios de computación en nube y los modelos de servicios en nube entran en el ámbito de aplicación de la Directiva (UE) 2022/2555 (la «Directiva SRI 2») ([28]), que establece requisitos de gestión de riesgos de ciberseguridad para los proveedores de servicios de computación en nube. Estos requisitos se especifican con más detalle en el Reglamento de Ejecución (UE) 2024/2690 de la Comisión ([29]).

8.1. **¿Qué se considera una solución de tratamiento de datos a distancia para un producto con elementos digitales?**

184. La definición de tratamiento de datos a distancia establecida en el artículo 3, punto 2, se basa en tres elementos: i) si el tratamiento de datos se realiza «a distancia»; ii) si la ausencia de dicho tratamiento de datos impediría que el producto con elementos digitales cumpliera alguna de sus funciones; y iii) si el programa informático ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad. Las tres subsecciones siguientes abordan cada uno de estos elementos en mayor profundidad.

([28]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza (DO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *La noción de «a distancia»*

185. La noción de «a distancia» a que se refiere el artículo 3, punto 2, es pertinente, pero no suficiente, para determinar si un producto con elementos digitales incluye soluciones de tratamiento de datos a distancia. Además, dada la variedad de soluciones que podrían incluirse en este concepto, no es posible proporcionar una definición exhaustiva de lo que significa «a distancia». Es necesaria una evaluación caso por caso por parte del fabricante.

186. El considerando 11 del Reglamento de Ciberresiliencia menciona los datos tratados o almacenados «a distancia por el fabricante» frente a los datos tratados o almacenados «localmente en el dispositivo del usuario». El tratamiento de datos a distancia suele tener lugar fuera del entorno del usuario de un producto con elementos digitales o del entorno operativo de una organización (en el caso de un usuario profesional). Sin embargo, esto no impide que el tratamiento también tenga lugar cerca del dispositivo («en el borde»). La transmisión de datos puede realizarse por cable (por ejemplo, cable ethernet) o de forma inalámbrica (por ejemplo, wifi o Bluetooth). La computación en la nube, incluida la computación en el borde, es un ejemplo típico del tratamiento de datos que tiene lugar «a distancia». Por ejemplo, en el caso de una función basada en la nube a la que el usuario accede desde una aplicación móvil, parte del tratamiento de datos tiene lugar en la nube, fuera del entorno del usuario.

187. Es importante señalar que las soluciones de tratamiento de datos a distancia no se ejecutan necesariamente en una infraestructura en la nube de terceros. El tratamiento de datos a distancia que se ejecute en servidores locales ubicados en las instalaciones del fabricante también puede constituir una solución de tratamiento de datos a distancia. En otras palabras, una solución que se ejecute en las instalaciones y en una nube privada tiene las mismas probabilidades de constituir una solución de tratamiento de datos a distancia que una solución que se ejecute en una nube pública y fuera de las instalaciones.

188. Las dos cuestiones decisivas y acumulativas que determinan si el tratamiento de datos está comprendido en el Reglamento de Ciberresiliencia como solución de tratamiento de datos a distancia se exponen a continuación, en las secciones *8.1.2* y *8.2*. En caso de respuesta afirmativa a ambas preguntas, el tratamiento de datos a distancia constituye una solución de tratamiento de datos a distancia.

8.1.2. *La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones?*

189. Tal como se establece en la definición de «tratamiento de datos a distancia» incluida en el artículo 3, punto 2, para que el tratamiento de datos a distancia pueda considerarse una solución de tratamiento de datos a distancia, su ausencia tendría que impedir que el producto con elementos digitales cumpliera alguna de sus funciones. El concepto de «funciones» incluido en esta definición no se limita a la «funcionalidad principal» o a la «finalidad prevista» del producto con elementos digitales, ya que el Reglamento de Ciberresiliencia no establece tal limitación. Las funciones incluidas en el ámbito de aplicación del Reglamento de Ciberresiliencia son tanto funciones que cumplen directamente la finalidad prevista del producto con elementos digitales tal como la experimentan los usuarios como las funciones que contribuyen al desempeño general del producto.

190. Algunos ejemplos de funciones en las que puede producirse el tratamiento de datos a distancia y que impedirían que un producto con elementos digitales cumpliera alguna de sus funciones serían: i) el envío de comandos a un dispositivo; ii) la sincronización de archivos; iii) la incorporación del usuario; iv) la configuración (personalización del producto con elementos digitales); v) la distribución automatizada de actualizaciones, incluida la actualización de funcionalidades y la aplicación de parches de seguridad; vi) la gestión de la identidad y el acceso.

191. En algunos casos, el usuario puede utilizar una función tanto a distancia como manualmente (por ejemplo, encender o apagar una bombilla mediante una aplicación o manualmente). El hecho de disponer de esta opción no excluye que el tratamiento de datos asociado a la ejecución a distancia de la función se considere una solución de tratamiento de datos a distancia. La ejecución de esta función a distancia también se considera parte de las funciones que ofrece el producto con elementos digitales.

192. En cambio, cuando la ausencia de un determinado tratamiento de datos no impida que el producto con elementos digitales cumpla alguna de sus funciones, dicho tratamiento no se considerará una solución de tratamiento de datos a distancia en el sentido del Reglamento de Ciberresiliencia. Esto incluye, por ejemplo, el análisis a distancia de datos de telemetría recopilados exclusivamente con fines estadísticos o para el desarrollo futuro del producto.

193. No obstante, incluso cuando el tratamiento de datos no contribuya al desempeño de una función de un producto con elementos digitales, es posible que los fabricantes tengan que considerar si dichos componentes remotos introducen riesgos para el producto con elementos digitales como parte de su evaluación de los riesgos de ciberseguridad (por ejemplo, a la luz del entorno operativo del producto) y mitigar dichos riesgos en consecuencia (por ejemplo, mediante medidas de mitigación a nivel del producto).

194. Los sitios web son un caso específico que merece más aclaraciones, como se explica asimismo en la sección *2.1* Introducción en el mercado. Los sitios web no entran en el ámbito de aplicación de las soluciones de tratamiento de datos a distancia cuando no contribuyen al desempeño de una función de un producto con elementos digitales, como se explica en el considerando 11 del Reglamento de Ciberresiliencia. No basta con que un sitio web contenga información sobre un producto con elementos digitales para que se considere que entra en el ámbito de aplicación de las soluciones de tratamiento de datos a distancia, aunque el producto redirija a dicho sitio web. Por ejemplo, redirigir a los usuarios a una página web externa que proporcione información e instrucciones a los usuarios no constituye una solución de tratamiento de datos a distancia. En cambio, un sitio web puede entrar en el ámbito de aplicación de las soluciones de tratamiento de datos a distancia si permite o da soporte a una función de un producto con elementos digitales. Por ejemplo, un portal de autenticación que emita credenciales o testigos de autenticación necesarios para el funcionamiento del producto con elementos digitales se consideraría una solución de tratamiento de datos a distancia, siempre que también se cumplan los demás criterios de la definición.

8.1.3. *El programa informático ¿ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad?*

195. La definición de «tratamiento de datos a distancia» del artículo 3, punto 2, del Reglamento de Ciberresiliencia especifica además que el programa informático de dicho tratamiento de datos a distancia debe ser diseñado y desarrollado por el fabricante, o bajo su responsabilidad. El tratamiento de datos a distancia desarrollado y diseñado íntegramente por el fabricante (internamente) constituiría naturalmente una solución de tratamiento de datos a distancia. Lo mismo sucedería cuando los fabricantes recurran a un proveedor de servicios externo para el desarrollo y el diseño de una solución (es decir, «bajo su responsabilidad»). La frase «bajo su responsabilidad» se refiere a soluciones de tratamiento a distancia diseñadas específicamente para el fabricante. Se trata de casos en los que el fabricante no se limita a conceder una licencia de un producto con elementos digitales o un servicio existente que un proveedor de servicios ofrece a sus clientes, ni de versiones de estos ligeramente modificadas. «[B] ajo su responsabilidad» implica que el programa informático lo desarrolla exclusivamente el fabricante, o por encargo de este, sobre la base de los diseños y las especificaciones proporcionados por este.

196. Para determinar si existe una solución de tratamiento de datos a distancia, no es determinante «quién utiliza la solución», ya que la definición de las soluciones de tratamiento de datos a distancia en el Reglamento de Ciberresiliencia solo hace referencia a su diseño y desarrollo. Esto es coherente con el enfoque del Reglamento de Ciberresiliencia, según el cual los requisitos y obligaciones recaen en los fabricantes, y no en la utilización del producto con elementos digitales. Si los fabricantes diseñan y desarrollan soluciones, que luego son utilizadas por un tercero, siguen siendo responsables del cumplimiento de los requisitos esenciales del Reglamento de Ciberresiliencia aplicables al producto con elementos digitales que introducen en el mercado.

197. Es necesario diferenciar entre los casos en los que el diseño y el desarrollo los realizan los fabricantes (o se realizan bajo su responsabilidad) y los casos en que se recurre a soluciones de terceros que no han sido diseñadas y desarrolladas por los fabricantes (o bajo su responsabilidad). A modo de ejemplo, conviene tener en cuenta los modelos de servicios en la nube más comunes que ofrecen distintos grados de control por parte del usuario y que también se citan en el considerando 12 del Reglamento de Ciberresiliencia, a saber, el software como servicio (SaaS), la plataforma como servicio (PaaS) y la infraestructura como servicio (IaaS).

198. En el caso de una solución IaaS de terceros, el fabricante no gestiona ni controla los recursos físicos y virtuales subyacentes (como el equipo informático subyacente y el hipervisor del proveedor de servicios en la nube), pero puede implementar y ejecutar programas informáticos arbitrarios utilizando dichos recursos, como sistemas operativos y aplicaciones. Estos programas informáticos son diseñados y desarrollados por el fabricante, o bajo su responsabilidad, por lo que pueden constituir una solución de tratamiento de datos a distancia, siempre que cumplan los demás elementos de la definición.

199. En el caso de una solución PaaS de terceros, el fabricante implementa su propia aplicación (creada o adquirida) utilizando lenguajes de programación y entornos de ejecución proporcionados por el proveedor de servicios en la nube e integra la aplicación en su producto con elementos digitales. El fabricante tiene control sobre la aplicación y, posiblemente, sobre los parámetros de configuración del entorno de ejecución. Por tanto, la aplicación es diseñada y desarrollada por el fabricante, o bajo su responsabilidad, por lo que puede constituir una solución de tratamiento de datos a distancia, siempre que cumpla los demás elementos de la definición.

200. En el caso de una solución SaaS de terceros, el proveedor de SaaS ofrece al fabricante una aplicación plenamente desarrollada para integrarla en el producto con elementos digitales del fabricante. El fabricante tiene una capacidad limitada para gestionar los parámetros de configuración de la aplicación específicos del usuario. Por tanto, la aplicación no es diseñada ni desarrollada por el fabricante ni bajo su responsabilidad.

201. No obstante, cuando determinados elementos no constituyan soluciones de tratamiento de datos a distancia (por ejemplo, el hipervisor en el caso de una infraestructura IaaS de terceros, el sistema operativo en el caso de una solución PaaS de terceros o la aplicación SaaS de terceros), pero estén integrados en el producto con elementos digitales de manera que afecten a su seguridad, dichas soluciones deben considerarse similares a los componentes de terceros. El fabricante está obligado a determinar y evaluar los riesgos relacionados con la integración de dichos elementos y a abordarlos aplicando los requisitos esenciales al propio producto con elementos digitales. Cuando proceda, esto puede verse respaldado por las funciones de seguridad que el proveedor de servicios en la nube pone a disposición a través de su modelo de responsabilidad compartida, cuando el fabricante utilice o confiera dichas funciones para hacer frente a los riesgos detectados. Además, se espera que el fabricante cumpla, en relación con la seguridad de estos componentes, una obligación similar a la obligación de ejercer la diligencia debida a que se refiere el artículo 13, apartado 5, de manera proporcionada al riesgo que la solución a distancia plantea para la seguridad del producto con elementos digitales.

202. Por lo tanto, puede resumirse que:

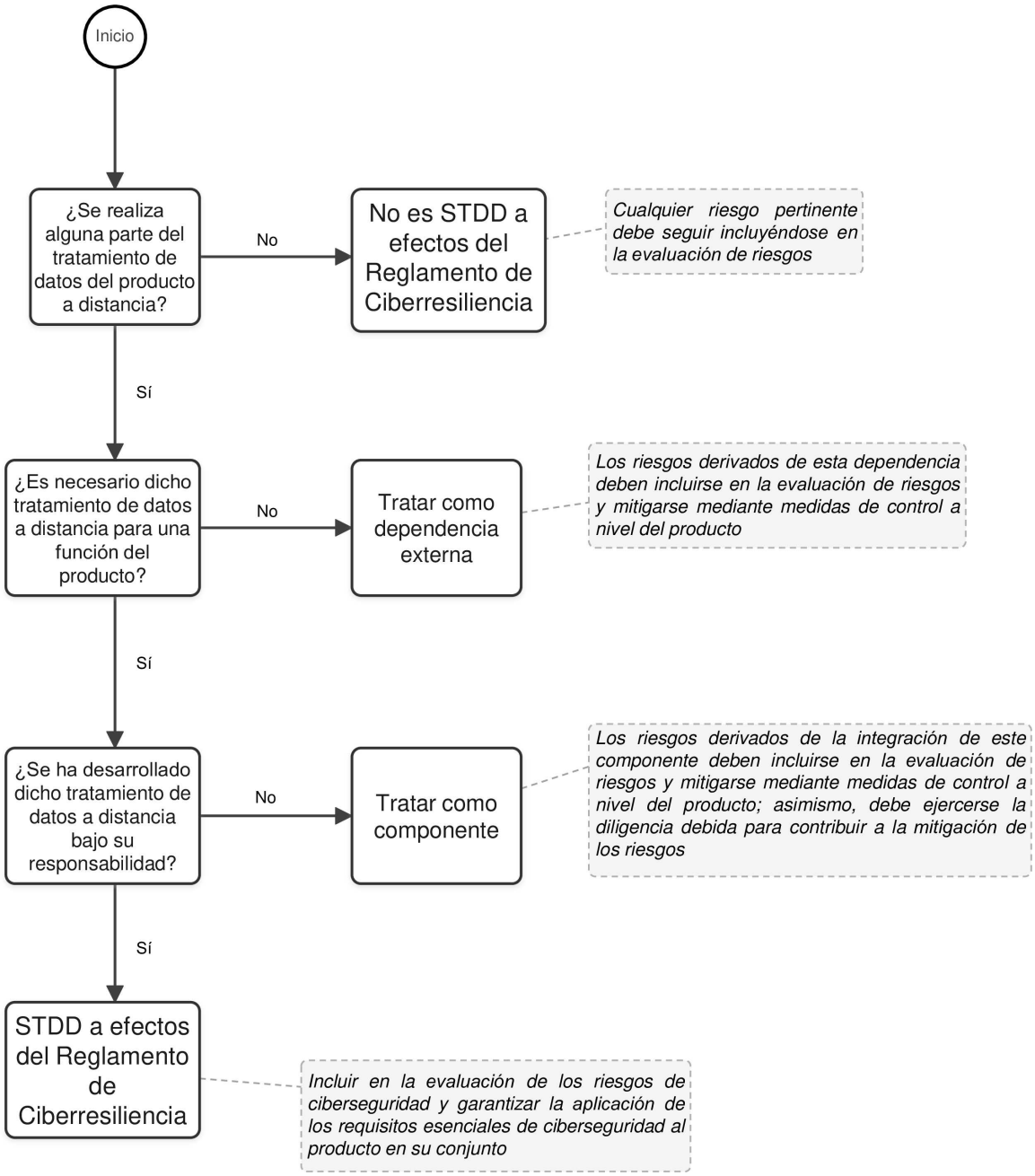
a) para que el tratamiento de datos se considere una solución de tratamiento de datos a distancia, la respuesta a las dos preguntas planteadas en las secciones *8.1.2* La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones? y *8.1.3* El programa informático ¿ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad? debe ser afirmativa;

b) si la respuesta a la pregunta de la sección *8.1.2* La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones? es negativa, los fabricantes deben evaluar los riesgos derivados de la existencia de dicho tratamiento de datos como parte de su evaluación de riesgos;

c) si la respuesta a la pregunta de la sección *8.1.2* La ausencia de dicho tratamiento de datos ¿impediría que el producto con elementos digitales cumpliera alguna de sus funciones? es afirmativa, pero la respuesta a la pregunta de la sección *8.1.3* El programa informático ¿ha sido diseñado y desarrollado por el fabricante, o bajo su responsabilidad? es negativa, los fabricantes deben tratar la solución de terceros como un componente. Como parte de la evaluación de riesgos, los fabricantes deben evaluar los riesgos derivados de la integración de dicha solución y mitigarlos en consecuencia. Además, los fabricantes deben ejercer la diligencia debida.

Gráfico 9:

diagrama de flujo esquematizado para determinar si un producto con elementos digitales contiene soluciones de tratamiento de datos a distancia (STDD)



8.2. Implicaciones prácticas y técnicas de las soluciones de tratamiento de datos a distancia y dependencia de soluciones de terceros

203. El Reglamento de Ciberresiliencia sigue un enfoque basado en los riesgos, consagrado en el artículo 13, apartados 2 y 3, así como en el primer requisito esencial de la parte I del anexo I, según el cual «[l]os productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes». Por consiguiente, debe aplicarse un enfoque basado en los riesgos a la hora de aplicar los requisitos del Reglamento de Ciberresiliencia a las soluciones de tratamiento de datos a distancia y al abordar los riesgos derivados de los servicios de terceros integrados en el producto con elementos digitales.

204. En primer lugar, los fabricantes deben i) indicar en la documentación técnica que su producto con elementos digitales dispone de una solución de tratamiento de datos a distancia o se basa en soluciones a distancia de terceros y ii) describir dichas soluciones. Si una misma solución de tratamiento de datos a distancia presta servicio a varios productos con elementos digitales, debe declararse dicha solución en la documentación técnica de cada producto. La documentación relativa a las soluciones de tratamiento de datos a distancia que prestan servicio a varios productos con elementos digitales podrá reutilizarse de una evaluación de la conformidad de un producto a otra.

205. Como se indica en el considerando 11, las soluciones de tratamiento de datos a distancia que forman parte del producto con elementos digitales y, por tanto, están sujetas a la evaluación de la conformidad del producto deben limitarse a aquellos módulos de programas informáticos responsables de la funcionalidad del producto con elementos digitales y a las interfaces que dichos módulos utilizan con servicios externos. Los sistemas *back-end* adicionales que lleven a cabo tratamientos posteriores y con los que el producto con elementos digitales no interactúe directamente no se consideran soluciones de tratamiento de datos a distancia.

206. No obstante, estos sistemas *back-end* siguen siendo dependencias externas que deben evaluarse como parte de la evaluación de los riesgos de ciberseguridad y mitigarse mediante medidas a nivel del producto. De hecho, la evaluación de riesgos realizada por el fabricante debe tener en cuenta: i) los riesgos relacionados con las soluciones de tratamiento de datos a distancia; ii) los riesgos relacionados con la dependencia de soluciones a distancia de terceros (de forma similar a los componentes de terceros); y iii) los riesgos relacionados con el entorno del producto (por ejemplo, el equipo informático subyacente). Los fabricantes deben aplicar controles de seguridad en el propio producto con elementos digitales para mitigar esos riesgos.

207. Además, como parte de la evaluación de la conformidad o del cumplimiento de las obligaciones de diligencia debida relacionadas con los servicios a distancia prestados por terceros, puede reutilizarse la siguiente lista no exhaustiva de elementos de garantía para respaldar la evaluación del fabricante:

a) pruebas del cumplimiento de las obligaciones establecidas en el Reglamento de Ejecución (UE) 2024/2690 de la Comisión;

b) pruebas del cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2022/2554;

c) declaración de conformidad o certificado obtenido en el marco de un esquema europeo de certificación de la ciberseguridad [adoptado en virtud del Reglamento (UE) 2019/881, «Reglamento sobre la Ciberseguridad»];

d) pruebas de conformidad con las normas ISO/IEC 27017:2015 o ISO/IEC 27001:2022.

208. Por último, en sus interacciones con proveedores terceros de servicios a distancia, los fabricantes deben aplicar las medidas de seguridad más adecuadas sobre la base de su evaluación de riesgos (y, cuando proceda, con el apoyo del modelo de responsabilidad compartida del proveedor). Dichas medidas de mitigación deben incluir controles de seguridad para sus productos con elementos digitales y la verificación de las medidas de seguridad proporcionadas por los propios proveedores terceros (diligencia debida). Una herramienta para mitigar estos riesgos puede consistir en incluir garantías de seguridad en sus acuerdos de nivel de servicio con los proveedores terceros, incluidas garantías de que los proveedores gestionan adecuadamente las vulnerabilidades. Un cambio importante en las soluciones proporcionadas por los proveedores terceros de servicios a distancia no debe constituir una modificación sustancial del producto con elementos digitales, ya que estos elementos no son responsabilidad del fabricante. Sin embargo, como parte de sus obligaciones de diligencia debida y para mitigar correctamente los riesgos derivados del uso de proveedores terceros, se recomienda a los fabricantes que se aseguren de que sus proveedores terceros de servicios en la nube los mantengan debidamente informados de los cambios que introduzcan en sus soluciones. Sobre la base de dicha información, es posible que los fabricantes tengan que revisar su evaluación de riesgos. La evaluación de riesgos actualizada debe determinar si los proveedores terceros de servicios siguen ofreciendo garantías suficientes en términos de ciberseguridad y si los controles de seguridad a nivel del producto siguen siendo adecuados. En algunos casos, los fabricantes pueden tener que modificar dichos controles o cambiar de proveedores terceros de servicios.

8.3. **Casos de uso de soluciones de tratamiento de datos a distancia**

Con el fin de proporcionar orientaciones prácticas adicionales a los fabricantes, esta sección recoge una serie de casos de uso ficticios en los que se describen los productos arquetípicos con elementos digitales que dependen del tratamiento de datos a distancia, y se analiza si dicho tratamiento constituye una solución de tratamiento de datos a distancia en el sentido del Reglamento de Ciberresiliencia.

8.3.1. *Aplicación de banca móvil*

Una entidad financiera introduce en el mercado una aplicación de banca móvil. Los sistemas *back-end* de la aplicación permiten, entre otras funciones, la autenticación, la autorización, la gestión de cuentas y los pagos. La entidad financiera utiliza una estrategia híbrida que se basa tanto en infraestructuras propias como en soluciones a distancia de terceros para dar soporte a las funcionalidades de la aplicación. Entre ellos, se incluyen los siguientes:

Infraestructura autoalojada desarrollada por la entidad financiera:

— El cliente abre la aplicación de banca móvil y se autentica a través de la interfaz bancaria, una solución autoalojada desarrollada por la entidad financiera que recibe las solicitudes de la aplicación y devuelve las respuestas correspondientes. La interfaz bancaria verifica la identidad del cliente consultando el sistema de gestión de cuentas y concede acceso a la aplicación.

— El cliente inicia una transferencia a través de la aplicación; la aplicación entonces transmite la instrucción a la interfaz bancaria, que envía la solicitud correspondiente al sistema de contabilidad.

— El sistema de gestión de cuentas y el sistema de contabilidad, ambos autoalojados pero lógicamente separados de la interfaz bancaria, registran la operación.

— El sistema de contabilidad devuelve el estado de la operación a la interfaz bancaria, que presenta el resultado al cliente.

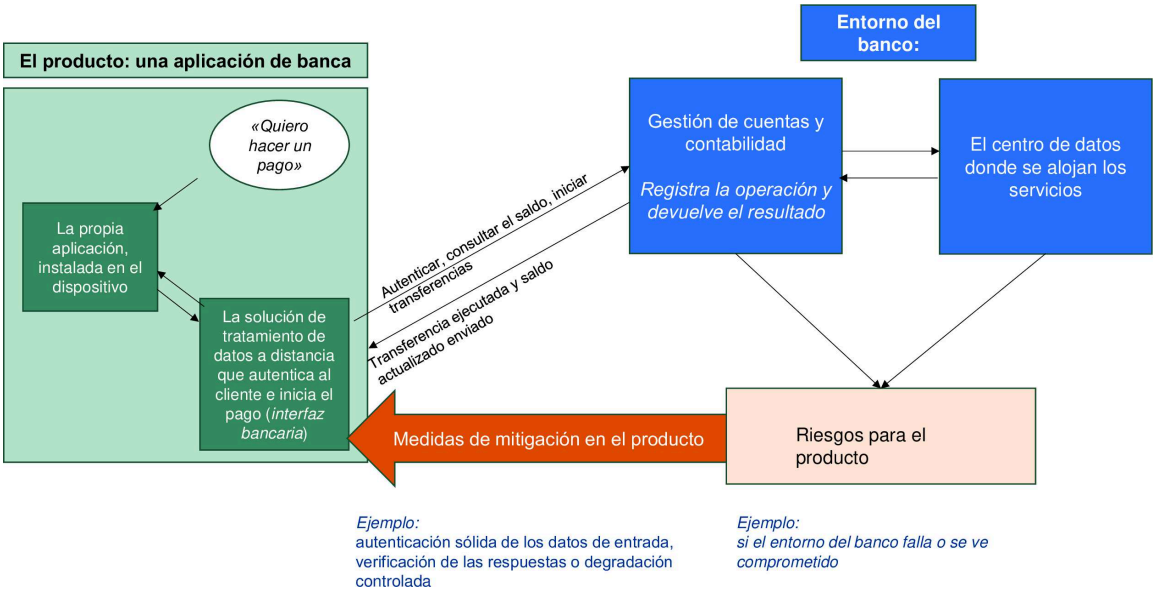
Implicaciones para las soluciones de tratamiento de datos a distancia:

— La interfaz bancaria es necesaria para que la aplicación desempeñe sus funciones, a saber, autenticar al cliente, transmitir las instrucciones del cliente, incluidas las instrucciones de pago y transferencia, y devolver el estado resultante. La interfaz bancaria se diseña y desarrolla bajo la responsabilidad del fabricante. Dado que la respuesta a las dos preguntas presentadas en las secciones anteriores es afirmativa, la interfaz bancaria constituye una solución de tratamiento de datos a distancia. Por tanto, debe incluirse en la evaluación de los riesgos de ciberseguridad y en la aplicación de los requisitos esenciales de ciberseguridad al producto con elementos digitales en su conjunto. El tratamiento posterior de una instrucción una vez transmitida, en particular el registro de la operación en los sistemas de gestión de cuentas y de contabilidad, liquidación y compensación, se lleva a cabo mediante sistemas con los que la aplicación no interactúa directamente, por lo que no constituye una solución de tratamiento de datos a distancia.

— El sistema de gestión de cuentas y el sistema de contabilidad no se consideran soluciones de tratamiento de datos a distancia para la aplicación de banca móvil. La aplicación no interactúa directamente con ellos (interactúa en su lugar con la interfaz bancaria, que a su vez depende de dichos sistemas). Aunque su disponibilidad puede ser necesaria para que se complete una función, el Reglamento de Ciberresiliencia solo se aplica a aquellas partes del sistema que interactúan directamente con el producto con elementos digitales. Por lo tanto, quedan fuera de la definición de solución de tratamiento de datos a distancia a efectos del Reglamento de Ciberresiliencia. Sin embargo, estos sistemas siguen siendo dependencias externas que pueden dar lugar a riesgos de ciberseguridad significativos para el producto con elementos digitales. Por ejemplo, si la seguridad del sistema de contabilidad se viera comprometida, podría permitir a un atacante influir en los resultados de las operaciones que se muestran posteriormente en la aplicación. Por lo tanto, el fabricante está obligado a determinar y evaluar dichos riesgos como parte de la evaluación de los riesgos de ciberseguridad y a mitigarlos mediante medidas a nivel del producto, como una autenticación reforzada de las interfaces de *back-end*, la protección de la integridad de los datos de las operaciones, canales de comunicación seguros y la verificación de las respuestas recibidas por la aplicación.

Gráfico10:

representación esquemática de una aplicación de banca que depende de soluciones de tratamiento de datos a distancia (STDD)



SaaS de terceros para la atención al cliente:

— La entidad financiera integra en su aplicación una solución de chat de atención al cliente desarrollada y gestionada por un proveedor tercero; dicho proveedor tercero ha escrito el código del servidor del chat, ha construido la interfaz de usuario y gestiona la infraestructura en la que se implanta el chat (es decir, el modelo SaaS).

— Cuando el cliente inicia una solicitud de atención, la aplicación conecta al cliente con el servicio de terceros para establecer una sesión de chat y gestionar el flujo de mensajes, sin proporcionar al tercero acceso a los sistemas bancarios esenciales.

Implicaciones para las soluciones de tratamiento de datos a distancia:

— La solución de chat de atención al cliente es necesaria para que el producto con elementos digitales cumpla alguna de sus funciones, pero no ha sido diseñada ni desarrollada por la entidad financiera ni bajo su responsabilidad; por lo tanto, no constituye una solución de tratamiento de datos a distancia. Sin embargo, debe tratarse como un componente de terceros. La dependencia de dicho servicio de terceros puede generar riesgos de ciberseguridad para la aplicación de banca, por ejemplo, si un atacante utilizara el canal de chat para suplantar al banco o para enviar contenido malicioso a los usuarios. La entidad financiera debe tener en cuenta dichos riesgos en su evaluación de los riesgos de ciberseguridad y mitigarlos mediante medidas a nivel del producto, como aislar la función de chat de las funcionalidades esenciales de banca, controlar los flujos de datos y validar el contenido. También debe ejercerse la diligencia debida respecto del SaaS.

8.3.2. *Termostato inteligente*

Un termostato inteligente permite a los usuarios controlar la temperatura de sus hogares a través de una aplicación móvil. La aplicación móvil y el termostato inteligente dependen del tratamiento de datos a distancia para intercambiar datos (por ejemplo, una solicitud para aumentar la temperatura) y almacenar datos (por ejemplo, las preferencias del usuario). Estas funciones se desarrollaron y diseñaron bajo la responsabilidad del fabricante, pero se ejecutan en una infraestructura física y virtual subyacente proporcionada por un tercero (IaaS de terceros).

Dado que el termostato inteligente no podría realizar sus funcionalidades inteligentes sin este tratamiento de datos a distancia, su ausencia impediría que el producto con elementos digitales realizara una o varias de sus funciones. Además, el programa informático se desarrolló y diseñó bajo la responsabilidad del fabricante del termostato inteligente. Por lo tanto, el tratamiento de datos a distancia constituye una solución de tratamiento de datos a distancia tal como se define en el Reglamento de Ciberresiliencia.

A efectos del cumplimiento del Reglamento de Ciberresiliencia, el fabricante del termostato inteligente debe documentar la solución de tratamiento de datos a distancia, así como la dependencia de la IaaS de terceros, en la documentación técnica del producto con elementos digitales, incluidos los datos relativos al servicio contratado. El fabricante debe tener en cuenta esos elementos en la evaluación de riesgos, que incluye la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales. El fabricante aplica los requisitos esenciales del Reglamento de Ciberresiliencia en función de los riesgos relacionados con la solución de tratamiento de datos a distancia. En el caso de la IaaS de terceros, el fabricante debe asegurarse de que las medidas de seguridad proporcionadas por el proveedor tercero sean adecuadas o adoptar las medidas pertinentes con respecto a la infraestructura. En el primer caso, el fabricante podría, por ejemplo, solicitar pruebas de que se han cumplido las obligaciones establecidas en la Directiva SRI 2.

8.3.3. *Lector de libros electrónicos*

El fabricante de un programa informático para un lector de libros electrónicos utiliza un servicio de almacenamiento SaaS de terceros para almacenar los libros electrónicos adquiridos por los clientes y permitirles acceder a ellos. La ausencia de este servicio de almacenamiento impediría que el producto con elementos digitales realizara una de sus funciones, pero el servicio de almacenamiento SaaS de terceros no ha sido desarrollado por el fabricante ni bajo su responsabilidad; el proveedor de SaaS lo pone a disposición de los clientes para cualquier caso de uso.

El servicio de almacenamiento SaaS no se ajusta a la definición de solución de tratamiento de datos a distancia. Sin embargo, el fabricante del lector de libros electrónicos depende de ese servicio externo para el funcionamiento de su producto con elementos digitales, por lo que debe tener en cuenta los riesgos asociados en su evaluación de los riesgos de ciberseguridad. El fabricante del lector de libros electrónicos debe tratar el SaaS como un componente. Asimismo, deberá aplicar medidas de seguridad adecuadas a nivel del producto, como la autenticación segura, el cifrado y la protección de la integridad de las comunicaciones con el servicio de almacenamiento. La diligencia debida a la hora de seleccionar e integrar al proveedor de SaaS también contribuirá al cumplimiento de las obligaciones del fabricante, de modo que el producto con elementos digitales en su conjunto cumpla los requisitos esenciales.

8.3.4. *Robot industrial*

Un robot industrial tiene la tarea de recoger piezas. El robot envía la información captada por las cámaras a un servicio a distancia diseñado y desarrollado por el fabricante. Este servicio se ejecuta en una infraestructura física y virtual subyacente proporcionada por un proveedor de servicios tercero (IaaS de terceros). El servicio en la nube calcula la posición de una pieza a partir de las imágenes captadas por las cámaras y envía comandos al robot para que recoja las piezas.

La ausencia de este tratamiento de datos impediría al robot industrial recoger las piezas y, en consecuencia, cumplir una de sus funciones. Además, el programa informático que se ejecuta sobre la infraestructura ha sido diseñado y desarrollado por el fabricante. El programa informático diseñado y desarrollado por el fabricante se ajusta a la definición de solución de tratamiento de datos a distancia.

El fabricante del robot industrial debe documentar la solución de tratamiento de datos a distancia, así como la dependencia de la IaaS de terceros, en la documentación técnica del producto con elementos digitales, incluidos los datos relativos al servicio contratado. El fabricante debe también tener en cuenta esos elementos en la evaluación de riesgos, que incluye la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales. El fabricante aplica los requisitos esenciales del Reglamento de Ciberresiliencia al producto con elementos digitales, incluida su solución de tratamiento de datos a distancia, en función de los riesgos. La diligencia debida a la hora de seleccionar al proveedor de la IaaS también contribuirá al cumplimiento de las obligaciones del fabricante. Por ejemplo, el fabricante podría solicitar pruebas de que se han cumplido las obligaciones establecidas en la Directiva SRI 2.

8.3.5. *Red de telefonía celular*

Un teléfono inteligente depende de una red 5G para proporcionar conexión a internet, llamadas telefónicas y mensajería a sus usuarios (conectividad móvil). La red de telefonía celular es desarrollada y diseñada por operadores de telecomunicaciones. La red comprende celdas pequeñas y torres de telefonía celular, así como otros equipos de red.

El producto con elementos digitales debe poder conectarse correctamente a una red; esta es una de sus funciones. Sin embargo, el hecho de que dicha red esté operativa o no, no es pertinente para determinar si el producto con elementos digitales funciona correctamente. La red es solo un canal de comunicación y no es necesaria para que el producto con elementos digitales cumpla su función de «conectarse correctamente a una red». Del mismo modo, un cable Ethernet, un enrutador o una señal wifi no se consideran un tratamiento de datos cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones, sino que permiten la comunicación o la conectividad.

En consecuencia, la red de telefonía celular no se ajusta a la definición de solución de tratamiento de datos a distancia. La red no debe considerarse un componente de terceros, ya que no existe ningún programa informático integrado en el producto con elementos digitales, sino que el producto simplemente depende de dicha red. Como tal, no es necesario que el fabricante cumpla las obligaciones de diligencia debida con respecto al proveedor de la red.

9. **ELEMENTOS ADICIONALES**

9.1. **Obligaciones de información**

209. De conformidad con el artículo 14, apartados 1 y 3, del Reglamento de Ciberresiliencia, un fabricante está obligado a notificar simultáneamente al CSIRT designado como coordinador y a la ENISA: i) cualquier vulnerabilidad aprovechada activamente presente en el producto con elementos digitales de la que tengan conocimiento; y ii) cualquier incidente grave que repercuta en la seguridad de un producto con elementos digitales del que tengan conocimiento.

210. De conformidad con el artículo 69, apartado 3, y el artículo 71, apartado 2, segunda frase, la obligación de cumplir lo dispuesto en el artículo 14 se aplicará a partir del 11 de septiembre de 2026 a todos los productos con elementos digitales que entren en el ámbito de aplicación del Reglamento de Ciberresiliencia, incluidos los productos con elementos digitales que se hayan introducido en el mercado antes del 11 de diciembre de 2027. Además, a diferencia de las obligaciones relativas a la gestión de las vulnerabilidades, que solo siguen siendo aplicables durante el período de soporte de un producto, las obligaciones de información siguen siendo aplicables una vez que un producto con elementos digitales ha dejado de recibir soporte. Cuando un producto con elementos digitales se haya introducido en el mercado antes del 11 de diciembre de 2027, o cuando su período de soporte haya finalizado, el fabricante no estará obligado a cumplir las obligaciones de gestión de las vulnerabilidades establecidas en la parte II del anexo I.

211. Cabe recordar que la obligación de notificar tales acontecimientos se aplica desde el momento en que el fabricante tiene conocimiento de que una vulnerabilidad está siendo aprovechada activamente o de que se ha producido un incidente grave que ha comprometido la seguridad de su producto con elementos digitales. Por lo tanto, las orientaciones sobre cuándo se considera que un fabricante ha tenido conocimiento de ello deben ayudar a los fabricantes a determinar el momento a partir del cual empiezan a correr los plazos de notificación aplicables.

212. Los fabricantes pueden estar sujetos a obligaciones de notificación comparables en virtud de diferentes actos de la UE. Para garantizar que la noción de «de la que tengan conocimiento» o «del que tengan conocimiento» se interprete de manera coherente y facilitar el cumplimiento de dichas obligaciones por parte de los fabricantes, las presentes orientaciones se ajustan al considerando 31 del Reglamento de Ejecución (UE) 2024/2690 de la Comisión y a la sección II, letra A), de las Directrices 9/2022 sobre la notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD.

213. En algunos casos, un fabricante detectará un acontecimiento sospechoso o un tercero, como un particular, un cliente, una entidad, una autoridad, una organización de medios de comunicación u otra fuente, pondrá en su conocimiento un posible incidente o vulnerabilidad. En tales casos, el fabricante debe evaluar el acontecimiento sospechoso de inmediato para determinar si constituye una vulnerabilidad aprovechada activamente o un incidente grave que repercute en la seguridad del producto con elementos digitales. Por lo tanto, se considerará que el fabricante ha tenido conocimiento de ello cuando, tras dicha evaluación inicial, tenga un grado razonable de certeza de que: i) se está aprovechando activamente una vulnerabilidad presente en su producto con elementos digitales; o ii) se ha producido un incidente grave que ha comprometido la seguridad de su producto con elementos digitales.

214. Por lo tanto, el momento a partir del cual puede considerarse que un fabricante tiene conocimiento de ello dependerá de las circunstancias de la vulnerabilidad aprovechada activamente o del incidente grave de que se trate. En algunos casos, quedará relativamente claro desde el principio que se está explotando activamente una vulnerabilidad o que un incidente grave está afectando a la seguridad de un producto con elementos digitales. En otros, puede llevar algún tiempo determinar si un producto con elementos digitales se ve afectado por una vulnerabilidad y si dicha vulnerabilidad está siendo aprovechada por un agente malintencionado, o bien si un incidente está afectando a la seguridad de un producto con elementos digitales. No obstante, debe hacerse hincapié en la necesidad de actuar con prontitud para llevar a cabo la evaluación inicial a fin de determinar si efectivamente se cumplen dichas condiciones, en particular cuando la vulnerabilidad pueda suponer un riesgo significativo, y, de ser así, adoptar medidas correctoras y notificarlas de conformidad con el Reglamento de Ciberresiliencia.

215. Además, la estructura de las obligaciones de información exige que los fabricantes actualicen progresivamente sus notificaciones, a medida que avanzan sus investigaciones internas y tienen un mayor conocimiento de la vulnerabilidad aprovechada activamente o del incidente. En particular, los fabricantes están obligados a presentar sin demora indebida y, en cualquier caso, en un plazo de 24 horas desde que hayan tenido conocimiento de ello, una notificación de alerta temprana que contenga información limitada. Posteriormente, se requiere información adicional como parte de la notificación que debe presentarse sin demora indebida y, en cualquier caso, en un plazo de 72 horas desde que hayan tenido conocimiento de ello («notificación en las 72 horas siguientes»). El informe completo debe presentarse en un plazo de 14 días desde que se disponga de una medida correctora o de mitigación para las vulnerabilidades aprovechadas activamente o, en el caso de incidentes graves, en el plazo de 1 mes desde la notificación en las 72 horas siguientes.

216. Como también se recuerda en la sección *3.3.1* Apoyo continuado y garantía de la viabilidad del programa informático libre y de código abierto, los administradores de comunidad de programas informáticos de código abierto también están obligados a notificar las vulnerabilidades aprovechadas activamente de conformidad con el artículo 24, apartado 3 ([30]). Esta obligación se aplica desde el momento en que se tiene conocimiento de una vulnerabilidad aprovechada activamente, y no simplemente cuando existe una vulnerabilidad en la base de código de un programa informático libre y de código abierto del que la entidad es administradora. En la práctica, dado que los componentes de programas informáticos libres y de código abierto suelen integrarse posteriormente en otros productos con elementos digitales, es probable que un administrador tenga conocimiento de la explotación activa a través de notificaciones de terceros, en las que se identifique la explotación de componentes de programas informáticos libres y de código abierto integrados en otros productos con elementos digitales. Este puede ser el caso, por ejemplo, cuando el fabricante de un producto con elementos digitales detecta una explotación activa de un componente de un programa informático libre y de código abierto integrado en su propio producto y lo notifica al administrador de dicho componente; o cuando un usuario o un investigador de seguridad encuentra pruebas de la explotación de un componente de un programa informático libre y de código abierto integrado en un producto con elementos digitales y notifica dicha explotación activa al administrador del componente.

217. También debe aclararse que, dado que la obligación de notificar las vulnerabilidades aprovechadas activamente se aplica cuando el fabricante tiene conocimiento de su aprovechamiento activo, este no está obligado a notificar las vulnerabilidades de cuyo aprovechamiento activo ya haya tenido conocimiento antes del 11 de septiembre de 2026 (fecha a partir de la cual comienza a aplicarse la obligación de información). Por lo tanto, el Reglamento de Ciberresiliencia no exige la notificación retroactiva de dichas vulnerabilidades. En cambio, la obligación sí se aplica en los casos en que el fabricante tuviera conocimiento de una vulnerabilidad antes del 11 de septiembre de 2026, pero en ese momento no tuviera conocimiento de que estuviera siendo aprovechada activamente (ya sea porque aún no se había producido ningún aprovechamiento activo o porque el fabricante aún no tenía conocimiento de él). Si, después del 11 de septiembre de 2026, se produce posteriormente un aprovechamiento activo o el fabricante tiene conocimiento de él, la vulnerabilidad se considera una vulnerabilidad aprovechada activamente sujeta a la obligación de información.

218. Del mismo modo, un fabricante solo está obligado a notificar las vulnerabilidades aprovechadas activamente contenidas en su producto con elementos digitales. Cuando un producto con elementos digitales contenga una vulnerabilidad aprovechada activamente que tenga su origen en un componente de terceros, el fabricante del producto con elementos digitales estará obligado a notificar dicha vulnerabilidad aprovechada activamente. No obstante, si un fabricante es consciente de que un componente de terceros contiene una vulnerabilidad, pero dicha vulnerabilidad i) no puede aprovecharse en su producto con elementos digitales (por ejemplo, porque no es posible acceder al código vulnerable) o ii) no ha sido aprovechada en su producto con elementos digitales, dicha vulnerabilidad no se considera una vulnerabilidad aprovechada activamente presente en su producto con elementos digitales y, por tanto, no está sujeta a la obligación de información para dicho fabricante. No obstante, el fabricante puede notificar dicha vulnerabilidad de forma voluntaria, de conformidad con el artículo 15 del Reglamento de Ciberresiliencia. Asimismo, debe cumplir los requisitos relativos a la gestión de las vulnerabilidades de la parte II del anexo I del Reglamento de Ciberresiliencia, así como notificar la vulnerabilidad a la persona o entidad que fabrica o mantiene el componente, de conformidad con el artículo 13, apartado 6, y como se explica con más detalle en la sección *9.2.1* Notificación *upstream* y puesta en común de las correcciones de seguridad.

([30]) En la medida en que el administrador participe en el desarrollo de un producto con elementos digitales.

219. Tras tener conocimiento de una vulnerabilidad aprovechada activamente o de un incidente grave, los fabricantes también están obligados, de conformidad con el artículo 14, apartado 8, a informar a los usuarios afectados y, en su caso, a todos los usuarios. Cuando no lo hagan a su debido tiempo, los CSIRT que hayan recibido la notificación podrán facilitar dicha información a los usuarios cuando se considere proporcionado y necesario para prevenir o mitigar las repercusiones de dicha vulnerabilidad o incidente.

220. En consonancia con el enfoque basado en los riesgos del Reglamento de Ciberresiliencia, la obligación de informar a los usuarios establecida en el artículo 14, apartado 8, debe aplicarse de manera proporcionada y basada en los riesgos. En particular, facilitar información sobre una vulnerabilidad aprovechada activamente o un incidente grave no implica que dicha información deba hacerse pública o divulgarse de forma indiscriminada. Cuando proceda, y a la luz de la naturaleza del producto con elementos digitales, de los usuarios afectados y de las posibles repercusiones de la vulnerabilidad o el incidente, los fabricantes pueden limitar la divulgación de información detallada a los usuarios o clientes pertinentes afectados. Este es el caso, en particular, de los productos con elementos digitales utilizados en entornos sensibles o esenciales, en los que la divulgación pública de detalles técnicos podría, por sí misma, aumentar los riesgos de ciberseguridad o facilitar que el aprovechamiento de la vulnerabilidad tenga una mayor repercusión.

221. Una vez que la vulnerabilidad se haya abordado o mitigado adecuadamente, puede resultar apropiado ampliar la divulgación. Este sería el caso, por ejemplo, cuando la divulgación contribuya a aumentar la sensibilización general o permita a los usuarios verificar que sus productos con elementos digitales ya no se ven afectados. En estos casos, el nivel de detalle y el momento en que se lleve a cabo cualquier divulgación más amplia deben seguir siendo proporcionados y tener en cuenta los riesgos residuales de explotación, la naturaleza del producto con elementos digitales y los intereses de los usuarios afectados. Además, el punto 4 de la parte II del anexo I exige a los fabricantes que hagan pública información sobre las vulnerabilidades subsanadas una vez que se haya puesto a disposición una actualización de seguridad.

9.2. **Gestión de las vulnerabilidades**

9.2.1. *Notificación* upstream *y puesta en común de las correcciones de seguridad*

222. El artículo 13, apartado 6, del Reglamento de Ciberresiliencia exige a los fabricantes que notifiquen las vulnerabilidades de los componentes integrados a la persona o entidad que fabrica o mantiene dicho componente (notificación *upstream*).

223. Los fabricantes solo están obligados a notificar *upstream* respecto de la versión del componente que integren. Cuando la persona o entidad que fabrica o mantiene el componente haya establecido políticas de seguridad, procesos coordinados de divulgación de vulnerabilidades o canales designados para notificar vulnerabilidades, deben efectuar la notificación de conformidad con dichas políticas, procesos o canales, en particular cuando la divulgación prematura de vulnerabilidades no subsanadas pueda aumentar los riesgos de ciberseguridad. Además, con el fin de reducir la carga para los encargados del mantenimiento *upstream*, especialmente en los proyectos de código abierto, los fabricantes no están obligados a notificar *upstream* cuando puedan confirmar que la persona o entidad que fabrica o mantiene un componente es consciente de la existencia de una vulnerabilidad. Se anima a los fabricantes a que adopten medidas razonables para evitar la presentación de notificaciones duplicadas, por ejemplo, comprobando las bases de datos de vulnerabilidades de acceso público, las recomendaciones de seguridad específicas de cada proyecto o sistemas de seguimiento de incidencias establecidos antes de notificar *upstream*.

224. Los fabricantes solo están obligados a notificar *upstream* respecto de las vulnerabilidades que existan en el propio componente integrado, y no respecto de las vulnerabilidades que existan como consecuencia de la integración del componente con otro código desarrollado por el fabricante o de la integración de otros componentes. No obstante, puede haber situaciones en las que la integración de un componente en un producto con elementos digitales específico revele determinados comportamientos, interacciones o características pertinentes para la seguridad de dicho componente que no fueran evidentes, o no fueran fácilmente identificables, de forma aislada. En tales casos, se recomienda a los fabricantes que comuniquen esta información a la persona o entidad que fabrica o mantiene el componente, con el fin de fomentar buenas prácticas de gestión de vulnerabilidades destinadas a facilitar una corrección eficaz y mejorar la seguridad general del ecosistema de componentes.

225. Por último, los fabricantes tampoco están obligados a notificar la vulnerabilidad *upstream* cuando el componente ya no tenga un encargado de su mantenimiento, o cuando el fabricante ya no dependa del encargado del mantenimiento original para nuevas versiones o correcciones de seguridad. No obstante, en tales casos, se recomienda a los fabricantes que informen a los usuarios de dicho componente a través de medidas alternativas razonables, por ejemplo, a través de los mecanismos comunitarios existentes (como listas de correo o tiques de incidencias) o mediante registros públicos de vulnerabilidades.

226. Además, de conformidad con el artículo 13, apartado 6, los fabricantes que hayan desarrollado una modificación de un programa informático para abordar una vulnerabilidad en un componente integrado están obligados a compartir dicha modificación del programa informático («corrección de seguridad») con la persona o entidad que fabrica o mantiene el componente («puesta en común *upstream*»).

227. Cuando se exija a los fabricantes compartir una corrección de seguridad con arreglo al artículo 13, apartado 6, la corrección debe facilitarse, cuando corresponda, en un formato legible por máquina, de manera que la persona o entidad que fabrica o mantiene el componente pueda verificarla fácilmente y, cuando proceda, integrarla. Cuando el componente sea un componente libre y de código abierto, la corrección de seguridad debe compartirse de manera compatible con la licencia de dicho componente, por ejemplo, con arreglo a la misma licencia o a una licencia que permita al encargado del mantenimiento distribuir la corrección con arreglo a su propia licencia. Cuando el encargado del mantenimiento de dicho componente disponga de directrices sobre cómo deben compartirse las correcciones de seguridad, el fabricante deberá seguir dichas directrices.

228. No obstante, el Reglamento de Ciberresiliencia no exige a los fabricantes que se aseguren de que sus correcciones de seguridad sean necesariamente aceptadas por la persona o entidad que fabrica o mantiene el componente. Tampoco están obligados a garantizar que dichas correcciones se integren necesariamente en el repositorio de código del componente, por ejemplo, cuando el encargado del mantenimiento prefiera una opción diferente para solucionar el problema. Del mismo modo, los fabricantes no están obligados a aceptar una corrección propuesta desarrollada por el encargado del mantenimiento del componente, y pueden preferir mitigar el problema de otras maneras adecuadas.

229. En algunos casos, la persona o entidad que fabrica o mantiene el componente puede haber proporcionado ya una corrección de seguridad para abordar la vulnerabilidad, pero un fabricante aplica una estrategia de mitigación diferente (por ejemplo, modificando una configuración diferente). En estos casos, el Reglamento de Ciberresiliencia no exige al fabricante que comparta *upstream* la modificación de otra parte del sistema. No obstante, se recomienda al fabricante que lo haga cuando ello pueda ayudar a la persona o entidad que mantiene el componente.

9.2.2. *Vulnerabilidades aprovechables conocidas*

230. Uno de los requisitos esenciales de la parte I del anexo I del Reglamento de Ciberresiliencia establece que, sobre la base de la evaluación de los riesgos de ciberseguridad a que se refiere el artículo 13, apartado 2, y cuando proceda, los productos con elementos digitales deben comercializarse sin vulnerabilidades aprovechables conocidas.

231. El artículo 3, punto 41, define la «vulnerabilidad aprovechable» como una «vulnerabilidad que puede ser utilizada de manera efectiva por un agente malintencionado en condiciones operativas prácticas». No todas las vulnerabilidades son aprovechables en condiciones operativas reales, y algunas vulnerabilidades solo son aprovechables en condiciones teóricas (por ejemplo, en un laboratorio o en una simulación) o en condiciones que no se darían en el entorno operativo de un producto con elementos digitales.

232. El Reglamento de Ciberresiliencia exige a los fabricantes que dispongan de políticas y procedimientos adecuados para gestionar y subsanar las posibles vulnerabilidades comunicadas por fuentes internas o externas (artículo 13, apartado 8). Sin embargo, no especifica explícitamente cuándo debe considerarse que el fabricante tiene conocimiento de una vulnerabilidad aprovechable, lo que da lugar a la obligación de cumplir este requisito esencial en el momento de la introducción en el mercado.

233. Debe considerarse que una vulnerabilidad es conocida cuando figure en las bases de datos de vulnerabilidades pertinentes de acceso público, como la base de datos europea de vulnerabilidades establecida en el artículo 12, apartado 2, de la Directiva (UE) 2022/2555 u otras bases de datos de vulnerabilidades de reconocido prestigio.

234. Además, una vulnerabilidad también puede considerarse conocida cuando el fabricante ha tenido conocimiento de ella a través de información no pública, por ejemplo, mediante una divulgación coordinada por parte de un investigador de seguridad o a través de las propias pruebas y análisis internos del fabricante, también, por ejemplo, cuando el fabricante utilice servicios basados en inteligencia artificial. Del mismo modo, una vulnerabilidad puede considerarse conocida cuando se haya informado de ella públicamente y de manera destacada en medios de comunicación fiables, entre ellos publicaciones especializadas en ciberseguridad o medios de comunicación generalistas.

235. No obstante, el mero hecho de que se notifique o detecte una vulnerabilidad no significa, por sí solo, que la vulnerabilidad sea aprovechable en la práctica o aplicable al producto con elementos digitales específico de que se trate. El fabricante tendrá que investigarla y confirmar la veracidad de dicha información y su aplicabilidad a su propio producto con elementos digitales. En consecuencia, puede transcurrir un período de tiempo limitado entre la primera notificación de la vulnerabilidad y su confirmación. Como se indica en la sección *9.1* Obligaciones de información, debe hacerse hincapié en la necesidad de actuar con prontitud para investigar y reaccionar a tiempo.

236. Por otro lado, la obligación de los fabricantes de cumplir los requisitos esenciales establecidos en la parte I del anexo I se aplica en el momento de la introducción en el mercado, de conformidad con el artículo 13, apartado 1. En la práctica, puede darse el caso de que se descubran nuevas vulnerabilidades potencialmente aprovechables durante las fases finales del ciclo de vida de desarrollo del producto con elementos digitales, incluso poco antes de que este entre en la cadena de distribución (y, por tanto, de que se introduzca en el mercado).

237. Dado que la obligación de introducir en el mercado productos con elementos digitales sin vulnerabilidades aprovechables conocidas es una obligación basada en los riesgos, corresponde al fabricante determinar si, sobre la base de la evaluación de los riesgos de ciberseguridad, es posible introducir el producto con elementos digitales en el mercado de forma segura y de conformidad con el Reglamento de Ciberresiliencia. Como alternativa, el fabricante puede determinar que es necesario subsanar una nueva vulnerabilidad de la que se haya podido tener conocimiento antes de que el producto con elementos digitales pueda introducirse en el mercado. Al tomar esta decisión, los fabricantes deben tener en cuenta la gravedad, la capacidad de explotación y el posible impacto de la vulnerabilidad, así como los riesgos que se planteen para el propio producto con elementos digitales una vez que esté en uso. También pueden tener en cuenta los riesgos de posponer la comercialización del producto hasta que se subsane la vulnerabilidad, por ejemplo, porque la nueva versión aborda asimismo otras vulnerabilidades aprovechables o porque es necesaria para garantizar el funcionamiento continuado de sistemas críticos. En cualquier caso, una vez que un producto con elementos digitales se ha introducido en el mercado, el fabricante sigue estando sujeto a la obligación de gestionar las vulnerabilidades de manera eficaz y de conformidad con los requisitos de gestión de las vulnerabilidades establecidos en la parte II del anexo I.

9.2.3. *Exámenes y pruebas eficaces y periódicos*

238. El punto 3 de la parte II del anexo I exige a los fabricantes que lleven a cabo exámenes y pruebas eficaces y periódicos del producto con elementos digitales durante todo su período de soporte. La realización de pruebas periódicas no requiere repetir mecánicamente, a intervalos fijos, una campaña de pruebas sin modificar. Esto significa que es necesario revisar periódicamente si nuevos datos, como amenazas detectadas o vulnerabilidades descubiertas recientemente, requieren que se actualicen las pruebas existentes, y realizar las pruebas en consecuencia.

239. La frecuencia, la profundidad y el contenido de la revisión deben ser proporcionales al perfil de riesgo de ciberseguridad del producto con elementos digitales, su evolución a lo largo del tiempo y el estado del panorama de amenazas. Cuando la revisión detecte nuevos datos pertinentes que afecten al conjunto de pruebas, deben diseñarse y realizarse nuevas pruebas o pruebas modificadas en el producto, a fin de garantizar que no queden vulnerabilidades sin abordar. Esto puede incluir volver a realizar pruebas existentes cuando una modificación del producto con elementos digitales haga adecuado este tipo de pruebas, como las pruebas de regresión.

240. Cuando la revisión no detecte ningún dato de este tipo, no será necesario diseñar pruebas adicionales. Las demás obligaciones relativas a la gestión de las vulnerabilidades, como la de abordar y subsanar las vulnerabilidades en relación con los riesgos planteados, siguen siendo aplicables en paralelo.

9.3. **Coherencia con otros actos legislativos**

9.3.1. *Reglamento (UE) 2019/2144 y Reglamento (UE) n.º 168/2013*

241. El artículo 2, apartado 2, letra c), del Reglamento de Ciberresiliencia establece que el Reglamento no se aplica a los productos con elementos digitales a los que se aplica el Reglamento (UE) 2019/2144. El Reglamento (UE) 2019/2144 se aplica a los «vehículos de las categorías M, N y O, tal como se definen en el artículo 4 del Reglamento (UE) 2018/858, y a los sistemas, componentes y unidades técnicas independientes diseñados y construidos para dichos vehículos».

242. Del mismo modo, los productos con elementos digitales que entran en el ámbito de aplicación del Reglamento (UE) n.º 168/2013 han sido excluidos del ámbito de aplicación del Reglamento de Ciberresiliencia mediante el Reglamento Delegado (UE) 2025/1535 de la Comisión. El Reglamento (UE) n.º 168/2013 se aplica a los vehículos de categoría L y «a los sistemas, componentes y unidades técnicas independientes, así como a las piezas y equipos diseñados y fabricados para tales vehículos» (artículo 2, apartado 1).

243. Los vehículos a los que se aplican dichos Reglamentos no están sujetos al Reglamento de Ciberresiliencia. Además, es necesario aclarar el alcance de la exención aplicable a los sistemas, componentes, unidades técnicas independientes, piezas y equipos (a efectos de la presente sección, «componentes») diseñados y fabricados para dichos vehículos que se consideren productos con elementos digitales en el sentido del Reglamento de Ciberresiliencia.

244. Se considera que dichos componentes no están sujetos al Reglamento de Ciberresiliencia, siempre que estén diseñados y fabricados exclusivamente para su integración en los vehículos incluidos en el ámbito de aplicación de los Reglamentos (UE) 2019/2144 y (UE) n.º 168/2013. Esto es así con independencia de que el fabricante de dicho componente lo venda directamente al fabricante del vehículo o a otro operador económico de la cadena de suministro del sector de la automoción, siempre que el componente esté claramente destinado y sea adecuado únicamente para su integración final en dichos vehículos.

245. En cambio, un fabricante que vende componentes genéricos que son productos con elementos digitales que pueden integrarse en diferentes tipos de productos, y no exclusivamente en vehículos incluidos en el ámbito de aplicación de dichos Reglamentos, está sujeto al Reglamento de Ciberresiliencia.

246. La evaluación de si un componente se introduce en el mercado en el sentido del Reglamento de Ciberresiliencia debe basarse en las condiciones objetivas en las que se pone a disposición. Cuando un fabricante ofrece un componente que no es exclusivamente adecuado para su integración final en dichos vehículos a través de canales de distribución abiertos a clientes ajenos a la cadena de suministro del sector de la automoción, como los puntos de venta al por menor en general o los canales de venta en línea que aceptan pedidos del público en general, entra en el ámbito de aplicación del Reglamento de Ciberresiliencia, con independencia de las declaraciones relativas a su uso previsto. En tales circunstancias, no puede considerarse que el componente se haya diseñado y fabricado exclusivamente para su integración en vehículos incluidos en el ámbito de aplicación de los Reglamentos (UE) 2019/2144 y (UE) n.º 168/2013, y el fabricante está obligado a cumplir el Reglamento de Ciberresiliencia. En cambio, el uso de canales de distribución restringidos a operaciones entre empresas y limitados a la cadena de suministro del sector de la automoción puede indicar que el componente se ha diseñado y fabricado exclusivamente para dicha integración.

9.3.2. *Validez de los certificados de examen de tipo UE (artículo 69, apartado 1)*

247. El artículo 69, apartado 1, establece que los certificados de examen de tipo UE y las decisiones de aprobación expedidos en relación con los requisitos de ciberseguridad para productos con elementos digitales que estén sujetos a otra legislación de armonización de la Unión distinta del presente Reglamento seguirán siendo válidos hasta el 11 de junio de 2028, salvo que caduquen con anterioridad a esa fecha o salvo que se indique lo contrario en esa legislación de armonización de la Unión, en cuyo caso seguirán siendo válidos según lo que disponga dicha legislación de la Unión.

248. La continuidad de la validez de dichos certificados y decisiones de aprobación debe entenderse limitada a los riesgos de ciberseguridad y los requisitos correspondientes contemplados en la respectiva legislación de armonización de la Unión sobre cuya base se hayan expedido. Para esos riesgos, los fabricantes no están obligados a volver a evaluar ni a demostrar de nuevo el cumplimiento únicamente a efectos del Reglamento de Ciberresiliencia durante el período de validez a que se refiere el artículo 69, apartado 1, en lo que respecta a los productos con elementos digitales que tengan intención de introducir en el mercado a partir del 11 de diciembre de 2027 y hasta el 11 de junio de 2028 ([31]). Este es el caso de los certificados y las decisiones de aprobación expedidos cuando la legislación de armonización de la Unión aplicable exige al fabricante que lleve a cabo el procedimiento de evaluación de la conformidad a través de un organismo notificado, así como cuando el fabricante ha optado voluntariamente por hacerlo.

249. En consecuencia, la existencia de un certificado o de una decisión de aprobación válidos en virtud de otra legislación de armonización de la Unión no exime a los fabricantes de llevar a cabo una evaluación exhaustiva de los riesgos de ciberseguridad con arreglo al Reglamento de Ciberresiliencia (ni de cumplir las demás obligaciones establecidas en él). Por el contrario, les permite basarse en las certificaciones existentes como prueba de conformidad a efectos de su procedimiento de evaluación de la conformidad, en la medida en que los riesgos de ciberseguridad correspondientes ya estén cubiertos. Cuando el certificado o la decisión de aprobación sean válidos con arreglo a otra legislación de armonización de la Unión que vaya más allá del 11 de junio de 2028, el fabricante podrá, no obstante, basarse en dicho certificado o decisión a efectos del Reglamento de Ciberresiliencia únicamente hasta el 11 de junio de 2028.

250. Cuando la evaluación de los riesgos de ciberseguridad realizada de conformidad con el artículo 13, apartado 2, detecte riesgos adicionales que no estén cubiertos por los requisitos de ciberseguridad en los que se basa el certificado o la decisión de aprobación existentes, los fabricantes seguirán siendo responsables de abordar dichos riesgos de conformidad con el Reglamento de Ciberresiliencia. En tales casos, el cumplimiento exige evaluar y mitigar las deficiencias detectadas, independientemente de que el certificado o la decisión de aprobación existentes sigan siendo válidos.

251. Esto puede ilustrarse considerando el caso de un producto con elementos digitales sujeto a los requisitos de ciberseguridad establecidos en el Reglamento Delegado (UE) 2022/30 de la Comisión, que complementa la Directiva 2014/53/UE (acto delegado de la Directiva sobre equipos radioeléctricos), y para el que se haya expedido un certificado de examen de tipo UE o una decisión de aprobación sobre la base de dichos requisitos. En este caso, el certificado o la decisión seguirán siendo válidos, de conformidad con el artículo 69, apartado 1, para los riesgos de ciberseguridad contemplados en dicho certificado y relacionados con los requisitos esenciales de ciberseguridad de la Directiva 2014/53/UE (Directiva sobre equipos radioeléctricos).

252. En tales casos, a efectos del Reglamento de Ciberresiliencia, los fabricantes no están obligados a volver a evaluar ni a demostrar de nuevo la conformidad con respecto a los riesgos que ya estén cubiertos por dichos certificados, mientras el certificado o la decisión de aprobación pertinentes sigan siendo válidos y, en cualquier caso, no más allá del 11 de junio de 2028. Esto incluye, por ejemplo, los riesgos de ciberseguridad relacionados con la protección de la red, la protección de los datos personales y la privacidad o la prevención del fraude (en la medida en que dichos riesgos estén contemplados en ese certificado) que estén relacionados con los requisitos de ciberseguridad de la Directiva sobre equipos radioeléctricos y se hayan tenido en cuenta en la evaluación de la conformidad.

253. Sin embargo, cuando la evaluación de los riesgos de ciberseguridad realizada de conformidad con el artículo 13, apartado 2, del Reglamento de Ciberresiliencia detecte riesgos adicionales que no estén cubiertos por los requisitos de ciberseguridad, los fabricantes seguirán siendo responsables de abordar dichos riesgos de conformidad con el Reglamento de Ciberresiliencia. Esto puede incluir, por ejemplo, los riesgos relacionados con los procesos de gestión de las vulnerabilidades, la minimización de datos y la reducción de la superficie de ataque, u otros aspectos de ciberseguridad específicos del producto que no se aborden en dichos certificados o que, en cualquier caso, no estén cubiertos por los requisitos esenciales de ciberseguridad de la Directiva sobre equipos radioeléctricos.

254. Por lo tanto, la existencia de un certificado de examen de tipo UE o de una decisión de aprobación válidos en virtud de la Directiva sobre equipos radioeléctricos para sus requisitos esenciales relativos a la ciberseguridad no demuestra, por sí sola, el pleno cumplimiento del Reglamento de Ciberresiliencia. Por el contrario, permite a los fabricantes basarse en dicho certificado o decisión como prueba del cumplimiento respecto de los riesgos correspondientes, garantizando al mismo tiempo que cualquier riesgo restante o que se haya identificado recientemente se evalúe y mitigue de conformidad con el Reglamento de Ciberresiliencia.

([31]) Los productos con elementos digitales introducidos en el mercado antes del 11 de diciembre de 2027 están sujetos a la legislación de la Unión aplicable en el momento de su introducción en el mercado y, si eran conformes en ese momento, pueden venderse y ponerse en funcionamiento, a menos que, a partir del 11 de diciembre de 2027, sean objeto de modificaciones sustanciales. Para los conceptos de «introducción en el mercado» y «comercialización», véase también la sección *2.1* Introducción en el mercado del presente documento, así como el capítulo 2 de la Guía azul.

255. Del mismo modo, cuando un producto con elementos digitales esté sujeto a los requisitos esenciales de salud y seguridad relacionados con la ciberseguridad establecidos en el Reglamento (UE) 2023/1230 (Reglamento relativo a las máquinas), que será plenamente aplicable a partir del 20 de enero de 2027, y cuando se haya expedido un certificado de examen de tipo UE o una decisión de aprobación sobre la base de dichos requisitos, dicho certificado o dicha decisión de aprobación seguirán siendo válidos, de conformidad con el artículo 69, apartado 1, del Reglamento de Ciberresiliencia, respecto de los riesgos de ciberseguridad contemplados en el Reglamento relativo a las máquinas.

256. En particular, esto afecta a los aspectos de ciberseguridad relacionados con la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de control, tal como se establece en las secciones 1.1.9 y 1.2.1 del anexo III del Reglamento relativo a las máquinas. Para esos riesgos, los fabricantes no están obligados a volver a evaluar ni a demostrar de nuevo la conformidad, mientras el certificado o la decisión de aprobación pertinentes sigan siendo válidos y, en cualquier caso, no más allá del 11 de junio de 2028. Esto se aplica en la medida en que dichos riesgos se hayan abordado como parte de la evaluación de la conformidad con arreglo al Reglamento relativo a las máquinas.

257. Al igual que en el caso de los requisitos esenciales de ciberseguridad de la Directiva sobre equipos radioeléctricos mencionados anteriormente, cuando la evaluación de los riesgos de ciberseguridad realizada con arreglo al artículo 13, apartado 2, del Reglamento de Ciberresiliencia identifique riesgos de ciberseguridad adicionales que no estén cubiertos por el certificado pertinente expedido con arreglo al Reglamento relativo a las máquinas y que estén relacionados con los requisitos de ciberseguridad de dicho Reglamento, los fabricantes seguirán siendo responsables de abordar dichos riesgos de conformidad con el Reglamento de Ciberresiliencia.