Parlamento Europeo
2019-2024

Comisión de Mercado Interior y Protección del Consumidor

2022/0272(COD)

30.6.2023

OPINIÓN

de la Comisión de Mercado Interior y Protección del Consumidor

para la Comisión de Industria, Investigación y Energía

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Ponente de opinión (*): Morten Løkkegaard

(*) Comisión asociada – artículo 57 del Reglamento interno

PA_Legam

BREVE JUSTIFICACIÓN

Como antiguo ponente de opinión en la Comisión IMCO sobre la Directiva SRI 2, el ponente percibe la Ley de ciberresiliencia como un siguiente paso crucial y natural para mejorar la ciberseguridad de la Unión Europea. Siendo plenamente conscientes de que, por definición, la ciberseguridad nunca será completa al 100 %, el ponente considera importante que hagamos todo lo que esté en nuestras manos para reducir el número de «eslabones débiles» existentes en nuestra Unión, y la Ley de ciberresiliencia constituye un paso adelante acogido favorablemente en esa dirección. Debemos reforzar la ciberseguridad de los productos con elementos digitales, así como de otros nuevos productos como los dispositivos del internet de las cosas que han pasado a constituir un componente natural de la vida ordinaria de los consumidores y las empresas europeos.

Habida cuenta de que la Comisión IMCO es responsable del funcionamiento y la implantación del mercado único, incluido el mercado único digital, y de las normas sobre la protección de los consumidores, el ponente ha procurado adoptar enmiendas encaminadas a mejorar el funcionamiento del mercado interior, proporcionando al mismo tiempo un elevado nivel de protección a los consumidores dentro del ámbito de aplicación de la propuesta, específicamente en lo que atañe a los requisitos de ciberseguridad de los productos con elementos digitales.

Además, el ponente cree que algunos aspectos de la propuesta de Reglamento deben mejorarse para generar claridad jurídica y coherencia entre las disposiciones pertinentes de dicha propuesta y otros instrumentos jurídicos, entre los que figuran, en particular, la Directiva SRI 2, el Reglamento relativo a la seguridad general de los productos recientemente adoptado, el Reglamento sobre la inteligencia artificial y el Reglamento relativo a las máquinas, así como diversos actos delegados y de ejecución pertinentes. En este sentido, el ponente ha propuesto enmiendas encaminadas a mejorar la claridad jurídica y a contribuir a garantizar una interpretación y una ejecución coherentes, eficaces y congruentes de los instrumentos referidos.

Por otra parte, dado que las microempresas y las pequeñas y medianas empresas son agentes económicos cruciales en el mercado digital, el ponente ha introducido varias enmiendas concebidas para simplificar los procedimientos administrativos y limitar la carga administrativa que soportan las pequeñas empresas, sin reducir el nivel de seguridad. El ponente ha introducido además varias enmiendas que garantizan que a las microempresas y a las pymes se les impartirán orientaciones y asesoramiento específicos para cumplir los requisitos de la Ley de ciberresiliencia.

Por último, el ponente ha introducido enmiendas con las que se pretende garantizar una comunicación más eficiente con las autoridades competentes (autoridades de vigilancia del mercado nacionales, ENISA), además de reforzar las disposiciones relativas a las obligaciones y a las competencias de las autoridades pertinentes en lo que atañe a las reclamaciones, las inspecciones y las actividades conjuntas. El ponente ha formulado asimismo algunas enmiendas centradas en la mejora de los requisitos de ciberseguridad para los componentes integrados en productos finales con elementos digitales, especificando las obligaciones de los operadores económicos, como los fabricantes y los representantes autorizados.

El ponente reitera la posición de que la adopción de la Ley de ciberresiliencia constituye un siguiente paso oportuno y natural para atajar las amenazas que se ciernen sobre la ciberseguridad en nuestra Unión. Con las enmiendas planteadas, el ponente ha procurado encontrar el equilibrio adecuado entre la consecución de un mayor nivel de ciberseguridad en beneficio de los consumidores europeos y una carga proporcionada para la comunidad empresarial. El ponente persigue que la ciberseguridad se convierta en un parámetro natural de la competencia en el mercado interior. El ponente ha procurado el ajuste de la propuesta con este objetivo en mente.

ENMIENDAS

La Comisión de Mercado Interior y Protección del Consumidor pide a la Comisión de Industria, Investigación y Energía, competente para el fondo, que tome en consideración las siguientes enmiendas:

Enmienda 1

Propuesta de Reglamento
Considerando 1

Texto de la Comisión	*Enmienda*
(1) Es necesario mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la comercialización de productos con elementos digitales en la Unión. Deben abordarse dos problemas importantes que suponen un aumento de los costes para los usuarios y la sociedad: un bajo nivel de ciberseguridad de los productos con elementos digitales, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y la insuficiencia de la comprensión de la información y del acceso a ella por parte de los usuarios, que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.	(1) Es necesario mejorar el funcionamiento del mercado interior ***procurando al mismo tiempo un nivel elevado de protección de los consumidores y de ciberseguridad*** mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la comercialización de productos con elementos digitales en la Unión. Deben abordarse dos problemas importantes que suponen un aumento de los costes para los usuarios y la sociedad: un bajo nivel de ciberseguridad de los productos con elementos digitales, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y la insuficiencia de la comprensión de la información y del acceso a ella por parte de los usuarios, que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

Enmienda 2

Propuesta de Reglamento
Considerando 7

Texto de la Comisión	*Enmienda*
(7) En determinadas condiciones, todos	(7) En determinadas condiciones, todos

los productos con elementos digitales integrados en un sistema electrónico de información más amplio o conectados a este pueden servir de vector de ataque para agentes malintencionados. En consecuencia, incluso los equipos y programas informáticos considerados menos críticos pueden facilitar que un dispositivo o red se vea comprometido en una fase inicial, lo que permite a los agentes malintencionados obtener un acceso privilegiado a un sistema o moverse lateralmente entre sistemas. Por consiguiente, los fabricantes deben garantizar que todos los productos con elementos digitales ***conectables*** se diseñen y desarrollen de conformidad con los requisitos esenciales establecidos en el presente Reglamento. Se incluyen aquí tanto los productos que puedan conectarse físicamente, a través de interfaces en los equipos informáticos, como los que se conecten mediante conexiones lógicas, a través, por ejemplo, de zócalos, conductos, archivos, interfaces de programación de aplicaciones o cualquier otro tipo de interfaz de programa. Teniendo en cuenta que las amenazas a la ciberseguridad pueden propagarse a través de diversos productos con elementos digitales antes de alcanzar un objetivo determinado, por ejemplo, mediante el aprovechamiento sucesivo de múltiples vulnerabilidades, los fabricantes también deben garantizar la ciberseguridad de aquellos productos cuya conexión a otros dispositivos o redes es indirecta.	los productos con elementos digitales integrados en un sistema electrónico de información más amplio o conectados a este pueden servir de vector de ataque para agentes malintencionados. En consecuencia, incluso los equipos y programas informáticos considerados menos críticos pueden facilitar que un dispositivo o red se vea comprometido en una fase inicial, lo que permite a los agentes malintencionados obtener un acceso privilegiado a un sistema o moverse lateralmente entre sistemas. Por consiguiente, los fabricantes deben garantizar que todos los productos con elementos digitales ***conectados a una red o un dispositivo externos*** se diseñen y desarrollen de conformidad con los requisitos esenciales establecidos en el presente Reglamento. Se incluyen aquí tanto los productos que puedan conectarse ***a redes o dispositivos externos*** físicamente, a través de interfaces en los equipos informáticos, como los que se conecten mediante conexiones lógicas, a través, por ejemplo, de zócalos, conductos, archivos, interfaces de programación de aplicaciones o cualquier otro tipo de interfaz de programa. Teniendo en cuenta que las amenazas a la ciberseguridad pueden propagarse a través de diversos productos con elementos digitales antes de alcanzar un objetivo determinado, por ejemplo, mediante el aprovechamiento sucesivo de múltiples vulnerabilidades, los fabricantes también deben garantizar la ciberseguridad de aquellos productos cuya conexión a otros dispositivos o redes es indirecta.

Enmienda 3

Propuesta de Reglamento
Considerando 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(7 bis) El presente Reglamento no debe aplicarse a las redes internas de un producto con elementos digitales si tales redes disponen de nodos finales dedicados y están completamente aisladas y protegidas frente a las conexiones de datos externas.

Enmienda 4

Propuesta de Reglamento
Considerando 7 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(7 ter) El presente Reglamento no debe aplicarse a las piezas de repuesto destinadas únicamente a sustituir piezas defectuosas de productos con elementos digitales con el fin de restablecer su funcionalidad.

Enmienda 5

Propuesta de Reglamento
Considerando 9

Texto de la Comisión	*Enmienda*
(9) El presente Reglamento garantiza un elevado nivel de ciberseguridad de los productos con elementos digitales. No regula servicios, como el software como servicio (SaaS)***, excepto en el caso de las soluciones de tratamiento de datos a distancia relacionadas con un producto con elementos digitales, entendido como todo tratamiento de datos a distancia para el que el programa informático haya sido diseñado y desarrollado por el fabricante del producto en cuestión o bajo la responsabilidad de dicho fabricante, y cuya ausencia impediría que el producto***	(9) El presente Reglamento garantiza un elevado nivel de ciberseguridad de los productos con elementos digitales. No regula servicios, como el software como servicio (SaaS). La [Directiva XXX/XXXX (SRI 2)] establece requisitos de ciberseguridad y de notificación de incidentes para las entidades esenciales e importantes, como las infraestructuras críticas, con el objetivo de aumentar la resiliencia de los servicios prestados. La [Directiva XXX/XXXX (SRI 2)] se aplica a los servicios de computación en nube y a los modelos de servicios en nube, como el

con elementos digitales cumpliera alguna de sus funciones. La [Directiva XXX/XXXX (SRI 2)] establece requisitos de ciberseguridad y de notificación de incidentes para las entidades esenciales e importantes, como las infraestructuras críticas, con el objetivo de aumentar la resiliencia de los servicios prestados. La [Directiva XXX/XXXX (SRI 2)] se aplica a los servicios de computación en nube y a los modelos de servicios en nube, como el SaaS. Todas las entidades que prestan servicios de computación en nube en la Unión y alcanzan o superan el umbral para las medianas empresas entran en el ámbito de aplicación de la Directiva.

SaaS. Todas las entidades que prestan servicios de computación en nube en la Unión y alcanzan o superan el umbral para las medianas empresas entran en el ámbito de aplicación de la Directiva.

Enmienda 6

Propuesta de Reglamento
Considerando 10

Texto de la Comisión	*Enmienda*
(10) Para no obstaculizar la innovación o la investigación, el presente Reglamento no debe aplicarse a los programas informáticos libres y de código abierto desarrollados o suministrados al margen de una actividad comercial. Este es el caso, en particular, de los programas informáticos, incluidos su código fuente y sus versiones modificadas, que se comparten abiertamente y son accesibles, utilizables, modificables y redistribuibles libremente. ***En el contexto de los programas informáticos,*** una actividad comercial puede caracterizarse ***no solo*** por la aplicación de un precio a un ***producto, sino*** también por la aplicación de un precio a los servicios de asistencia técnica, por el suministro de una plataforma de software a través de la cual el fabricante monetiza otros servicios o por el uso de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa	(10) ***Los programas informáticos y los datos que se compartan abiertamente y a los que los usuarios puedan acceder, usar, modificar y redistribuir con libertad (ya sean estos o versiones modificadas de los mismos) pueden contribuir a la investigación e innovación en el mercado. Los estudios llevados a cabo por la Comisión también ponen de relieve que los programas informáticos libres y de código abierto pueden aportar al PIB de la Unión entre 65 000 y 95 000 millones EUR, y que pueden proporcionar oportunidades de crecimiento significativas a la economía europea.*** Para no obstaculizar la innovación o la investigación, el presente Reglamento no debe aplicarse a los programas informáticos libres y de código abierto desarrollados o suministrados al margen de una actividad comercial. Este es el caso, en particular, de los programas informáticos, incluidos su código fuente y sus versiones modificadas, que se comparten

informático.	abiertamente y son accesibles, utilizables, modificables y redistribuibles libremente. ***No obstante***, una actividad comercial***, entendida como la introducción de un determinado producto o servicio en el mercado,*** puede caracterizarse por la aplicación de un precio a un ***componente de un programa informático libre y de código abierto***, pero también por ***actividades de monetización como*** la aplicación de un precio a los servicios de asistencia técnica, ***por las actualizaciones de programas informáticos retribuidas, a menos que tenga por finalidad únicamente la recuperación de los costes reales,*** por el suministro de una plataforma de software a través de la cual el fabricante monetiza otros servicios o por el uso de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático. ***Ni el desarrollo colaborativo de componentes de programas informáticos libres y de código abierto ni su puesta a disposición en repositorios abiertos deben constituir actividades de comercialización o puesta en servicio. Las circunstancias en las que se ha desarrollado el producto 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. Cuando un programa informático de código abierto se integra en un producto final con elementos digitales que se comercializa, el operador económico que haya comercializado dicho producto final será responsable de la conformidad del producto, incluidos los componentes libres y de código abierto.***

Enmienda 7

Propuesta de Reglamento
Considerando 11

Texto de la Comisión	*Enmienda*
(11) Una internet segura es indispensable para el funcionamiento de las infraestructuras críticas y para la sociedad en su conjunto. La [Directiva XXX/XXXX (SRI 2)] tiene por objeto garantizar un elevado nivel de ciberseguridad de los servicios prestados por entidades esenciales e importantes, incluidos los proveedores de infraestructuras digitales que apoyan las funciones básicas de la internet abierta o garantizan el acceso a internet y los servicios de internet. Por consiguiente, es importante que los productos con elementos digitales necesarios para que los proveedores de infraestructuras digitales garanticen el funcionamiento de internet se desarrollen de manera segura y cumplan normas de seguridad de internet bien establecidas. El presente Reglamento, que se aplica a todos los productos ***conectables*** consistentes en equipos y programas informáticos, tiene también por objeto facilitar que los proveedores de infraestructuras digitales cumplan los requisitos de la cadena de suministro con arreglo a la [Directiva XXX/XXXX (SRI 2)], garantizando que los productos con elementos digitales que utilizan para prestar sus servicios se desarrollen de forma segura y que tienen acceso a actualizaciones de seguridad oportunas para dichos productos.	(11) Una internet segura es indispensable para el funcionamiento de las infraestructuras críticas y para la sociedad en su conjunto. La [Directiva XXX/XXXX (SRI 2)] tiene por objeto garantizar un elevado nivel de ciberseguridad de los servicios prestados por entidades esenciales e importantes, incluidos los proveedores de infraestructuras digitales que apoyan las funciones básicas de la internet abierta o garantizan el acceso a internet y los servicios de internet. Por consiguiente, es importante que los productos con elementos digitales necesarios para que los proveedores de infraestructuras digitales garanticen el funcionamiento de internet se desarrollen de manera segura y cumplan normas de seguridad de internet bien establecidas. El presente Reglamento, que se aplica a todos los productos consistentes en equipos y programas informáticos ***conectados a una red o un dispositivo externos***, tiene también por objeto facilitar que los proveedores de infraestructuras digitales cumplan los requisitos de la cadena de suministro con arreglo a la [Directiva XXX/XXXX (SRI 2)], garantizando que los productos con elementos digitales que utilizan para prestar sus servicios se desarrollen de forma segura y que tienen acceso a actualizaciones de seguridad oportunas para dichos productos.

Enmienda 8

Propuesta de Reglamento
Considerando 15

Texto de la Comisión	*Enmienda*
(15) El Reglamento Delegado (UE) 2022/30 especifica que los requisitos esenciales establecidos en el artículo 3, apartado 3, letra d) (daños a la red y	(15) El Reglamento Delegado (UE) 2022/30 especifica que los requisitos esenciales establecidos en el artículo 3, apartado 3, letra d) (daños a la red y

utilización inadecuada de los recursos de la red), letra e) (datos personales y privacidad) y letra f) (fraude) de la Directiva 2014/53/UE se aplican a determinados equipos radioeléctricos. [La Decisión de Ejecución XXX/2022 de la Comisión relativa a una petición de normalización dirigida a las organizaciones europeas de normalización] establece requisitos para la elaboración de normas específicas que detallan con mayor precisión cómo deben abordarse estos tres requisitos esenciales. Los requisitos esenciales establecidos por el presente Reglamento incluyen todos los elementos de los requisitos esenciales mencionados en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE. Además, los requisitos esenciales establecidos en el presente Reglamento se ajustan a los objetivos de los requisitos de las normas específicas incluidos en dicha petición de normalización. Por tanto, ***si*** la Comisión ***deroga o modifica*** el Reglamento Delegado (UE) 2022/30 y, en consecuencia, este ***deja*** de aplicarse a determinados productos sujetos al presente Reglamento, la Comisión y las organizaciones europeas de normalización deben tener en cuenta el trabajo de normalización llevado a cabo en el contexto de la Decisión de Ejecución C(2022)5637 de la Comisión, relativa a una petición de normalización para el Reglamento Delegado (UE) 2022/30, que completa la Directiva sobre equipos radioeléctricos, en lo que respecta a la preparación y el desarrollo de normas armonizadas para facilitar la ejecución del presente Reglamento.

utilización inadecuada de los recursos de la red), letra e) (datos personales y privacidad) y letra f) (fraude) de la Directiva 2014/53/UE se aplican a determinados equipos radioeléctricos. [La Decisión de Ejecución XXX/2022 de la Comisión relativa a una petición de normalización dirigida a las organizaciones europeas de normalización] establece requisitos para la elaboración de normas específicas que detallan con mayor precisión cómo deben abordarse estos tres requisitos esenciales. Los requisitos esenciales establecidos por el presente Reglamento incluyen todos los elementos de los requisitos esenciales mencionados en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE. Además, los requisitos esenciales establecidos en el presente Reglamento se ajustan a los objetivos de los requisitos de las normas específicas incluidos en dicha petición de normalización. Por tanto, ***cuando*** la Comisión ***derogue*** el Reglamento Delegado (UE) 2022/30 y, en consecuencia, este ***deje*** de aplicarse a determinados productos sujetos al presente Reglamento, la Comisión y las organizaciones europeas de normalización deben tener en cuenta el trabajo de normalización llevado a cabo en el contexto de la Decisión de Ejecución C(2022)5637 de la Comisión, relativa a una petición de normalización para el Reglamento Delegado (UE) 2022/30, que completa la Directiva sobre equipos radioeléctricos, en lo que respecta a la preparación y el desarrollo de normas armonizadas para facilitar la ejecución del presente Reglamento.

Enmienda 9

Propuesta de Reglamento
Considerando 18 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(18 bis) Con el fin de garantizar que los desarrolladores individuales o microdesarrolladores de programas informáticos, tal como se definen en la Recomendación 2003/361/CE de la Comisión, no se enfrenten a importantes obstáculos financieros y no desistan de analizar la prueba de concepto, así como la justificación económica en el mercado, se debe exigir a estas entidades que hagan cuanto esté en su mano por cumplir con los requisitos de la presente propuesta durante los seis meses siguientes a la comercialización de un programa informático. Este régimen especial debe evitar el efecto disuasorio que unos elevados costes de conformidad y de entrada en el mercado podrían ejercer en los emprendedores y los particulares cualificados que consideren la opción de desarrollar programas informáticos en la Unión. Sin embargo, este régimen especial no debe aplicarse a los productos altamente críticos con elementos digitales.

Enmienda 10

Propuesta de Reglamento
Considerando 19

Texto de la Comisión	*Enmienda*
(19) De conformidad con el artículo 3, apartado 2, del Reglamento (UE) 2019/881, corresponde a la ENISA desempeñar determinadas tareas previstas en el presente Reglamento. En particular, la ENISA debe recibir notificaciones de los fabricantes relativas a las vulnerabilidades aprovechadas activamente presentes en los productos con elementos digitales y a los incidentes que repercutan en la seguridad de dichos productos. La ENISA también debe transmitir estas notificaciones a los equipos de respuesta a incidentes de	(19) De conformidad con el artículo 3, apartado 2, del Reglamento (UE) 2019/881, corresponde a la ENISA desempeñar determinadas tareas previstas en el presente Reglamento. En particular, la ENISA debe recibir notificaciones de los fabricantes***, mediante una alerta temprana,*** relativas a las vulnerabilidades aprovechadas activamente presentes en los productos con elementos digitales y a los incidentes que repercutan ***significativamente*** en la seguridad de dichos productos. La ENISA también debe

seguridad informática (CSIRT) pertinentes o, según corresponda, a los puntos de contacto únicos de los Estados miembros designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como informar a las autoridades de vigilancia del mercado pertinentes sobre la vulnerabilidad notificada. Sobre la base de la información que recopile, la ENISA debe elaborar un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en productos con elementos digitales y presentarlo al Grupo de Cooperación especificado en la Directiva [Directiva XXX/XXXX (SRI 2)]. Además, teniendo en cuenta sus conocimientos técnicos y su mandato, la ENISA debe poder apoyar el proceso de ejecución del presente Reglamento. En particular, debe ser capaz de proponer actividades conjuntas que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre el posible incumplimiento del presente Reglamento por parte de productos con elementos digitales en varios Estados miembros, o de identificar categorías de productos para las que deban organizarse acciones de control simultáneas coordinadas. En circunstancias excepcionales que requieran una intervención inmediata para preservar el buen funcionamiento del mercado interior, la ENISA, a petición de la Comisión, debe poder llevar a cabo evaluaciones relativas a productos específicos con elementos digitales que presenten un riesgo de ciberseguridad significativo.

transmitir estas notificaciones a los equipos de respuesta a incidentes de seguridad informática (CSIRT) pertinentes o, según corresponda, a los puntos de contacto únicos de los Estados miembros designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como informar ***inmediatamente*** a las autoridades de vigilancia del mercado pertinentes sobre la ***existencia de una vulnerabilidad y, cuando proceda, de las posibles medidas de mitigación del riesgo. Si para una*** vulnerabilidad notificada ***no hay disponibles medidas correctoras o de mitigación disponibles, la ENISA debe velar por que la información sobre la vulnerabilidad notificada se comunique en línea con unos estrictos protocolos de seguridad y según la necesidad de conocerla***. Sobre la base de la información que recopile, la ENISA debe elaborar un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en productos con elementos digitales y presentarlo al Grupo de Cooperación especificado en la Directiva [Directiva XXX/XXXX (SRI 2)]. Además, teniendo en cuenta sus conocimientos técnicos y su mandato, la ENISA debe poder apoyar el proceso de ejecución del presente Reglamento. En particular, debe ser capaz de proponer actividades conjuntas que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre el posible incumplimiento del presente Reglamento por parte de productos con elementos digitales en varios Estados miembros, o de identificar categorías de productos para las que deban organizarse acciones de control simultáneas coordinadas. En circunstancias excepcionales que requieran una intervención inmediata para preservar el buen funcionamiento del mercado interior, la ENISA, a petición de la Comisión, debe poder llevar a cabo evaluaciones relativas a productos específicos con elementos

digitales que presenten un riesgo de ciberseguridad significativo.

Enmienda 11

Propuesta de Reglamento
Considerando 20

Texto de la Comisión	*Enmienda*
(20) Los productos con elementos digitales deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado de productos con elementos digitales que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.	(20) Los productos con elementos digitales deben llevar el marcado CE para acreditar ***de manera visible, legible e indeleble*** su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado de productos con elementos digitales que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

Enmienda 12

Propuesta de Reglamento
Considerando 22

Texto de la Comisión	*Enmienda*
(22) A fin de garantizar que los productos con elementos digitales no planteen riesgos de ciberseguridad para las personas y las organizaciones al ser introducidos en el mercado, deben establecerse requisitos esenciales para dichos productos. Cuando estos se modifiquen posteriormente, por medios físicos o digitales, de una manera no prevista por el fabricante y que pueda implicar que dejen de cumplir los requisitos esenciales pertinentes, dicha modificación deberá considerarse sustancial. Por ejemplo, las actualizaciones de los programas informáticos o las reparaciones pueden ser incluidas entre las	(22) A fin de garantizar que los productos con elementos digitales no planteen riesgos de ciberseguridad para las personas y las organizaciones al ser introducidos en el mercado, deben establecerse requisitos esenciales para dichos productos. Cuando estos se modifiquen posteriormente, por medios físicos o digitales, de una manera no prevista por el fabricante y que pueda implicar que dejen de cumplir los requisitos esenciales pertinentes, dicha modificación deberá considerarse sustancial. Por ejemplo, las actualizaciones de los programas informáticos o las reparaciones***, como los ajustes menores***

operaciones de mantenimiento siempre que no modifiquen un producto ya introducido en el mercado de tal manera que puedan afectar a su observancia de los requisitos vigentes o cambiar el uso previsto para el cual se ha evaluado el producto. Al igual que en el caso de las reparaciones o modificaciones físicas, un producto con elementos digitales debe considerarse sustancialmente modificado por un cambio en los programas informáticos cuando la actualización de los programas informáticos modifique las funciones, el tipo o las prestaciones del producto previstos originalmente y ese cambio no estuviese previsto en la evaluación inicial del riesgo; o cuando la naturaleza del peligro haya cambiado o el nivel de riesgo haya aumentado debido a la actualización de los programas informáticos.

del código fuente que puedan mejorar la seguridad y el funcionamiento, pueden ser incluidas entre las operaciones de mantenimiento siempre que no modifiquen un producto ya introducido en el mercado de tal manera que puedan afectar a su observancia de los requisitos vigentes o cambiar el uso previsto para el cual se ha evaluado el producto. Al igual que en el caso de las reparaciones o modificaciones físicas, un producto con elementos digitales debe considerarse sustancialmente modificado por un cambio en los programas informáticos cuando la actualización de los programas informáticos modifique las funciones, el tipo o las prestaciones del producto previstos originalmente y ese cambio no estuviese previsto en la evaluación inicial del riesgo; o cuando la naturaleza del peligro haya cambiado o el nivel de riesgo haya aumentado debido a la actualización de los programas informáticos.

Enmienda 13

Propuesta de Reglamento
Considerando 23

Texto de la Comisión	*Enmienda*
(23) En consonancia con la noción comúnmente establecida de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, cada vez que se produzca una modificación sustancial que pueda afectar al cumplimiento del presente Reglamento por parte del producto o cuando la finalidad prevista del producto cambie, conviene que se verifique la conformidad del producto con elementos digitales y que, cuando proceda, se ***someta a una nueva*** evaluación de la conformidad. En su caso, si el fabricante lleva a cabo una evaluación de la conformidad en la que participa un tercero, deben notificarse a este último los cambios que puedan dar lugar a	(23) En consonancia con la noción comúnmente establecida de «modificación sustancial» de los productos regulados por la legislación de armonización de la Unión, cada vez que se produzca una modificación sustancial que pueda afectar al cumplimiento del presente Reglamento por parte del producto o cuando la finalidad prevista del producto cambie, conviene que se verifique la conformidad del producto con elementos digitales y que, cuando proceda, se ***actualice la*** evaluación de la conformidad. En su caso, si el fabricante lleva a cabo una evaluación de la conformidad en la que participa un tercero, deben notificarse a este último los cambios que puedan dar lugar a modificaciones

modificaciones sustanciales.	sustanciales. ***La evaluación de conformidad posterior debe abordar los cambios que dieron lugar a la nueva evaluación, salvo que tales cambios ejerzan un efecto significativo en la conformidad de otras partes del producto. Cuando se ejecuten actualizaciones de programas informáticos, el fabricante no debe estar obligado a efectuar otra evaluación de conformidad del producto con elementos digitales, salvo que la actualización de que se trate dé lugar a una modificación sustancial de dicho producto con elementos digitales.***

Enmienda 14

Propuesta de Reglamento
Considerando 24 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(24 bis) Los fabricantes de productos con elementos digitales deben garantizar que las actualizaciones de los programas informáticos se proporcionen de una forma clara y transparente, y diferenciar con claridad entre actualizaciones de seguridad y de funcionalidad. Si bien las actualizaciones de seguridad están diseñadas para reducir el nivel de riesgo de un producto con elementos digitales, la adopción de las actualizaciones de funcionalidad que ofrezca el fabricante debe seguir siendo siempre una opción para el usuario. Por tanto, los fabricantes deben ofrecer estas actualizaciones por separado, salvo que técnicamente resulte inviable. Los fabricantes deben proporcionar a los consumidores información adecuada sobre los motivos de cada actualización y su impacto previsto en el producto, así como un mecanismo de exclusión voluntaria claro y fácil de usar.

Enmienda 15

Propuesta de Reglamento
Considerando 25

Texto de la Comisión	*Enmienda*
(25) Los productos con elementos digitales deben considerarse críticos si las consecuencias negativas del aprovechamiento de posibles vulnerabilidades de ciberseguridad en el producto pueden ser graves debido a, entre otras cosas, su funcionalidad relacionada con la ciberseguridad o su uso previsto. En particular, las vulnerabilidades de los productos con elementos digitales cuya funcionalidad está relacionada con la ciberseguridad, como los elementos seguros, pueden llevar a que los problemas de seguridad se propaguen a lo largo de la cadena de suministro. La gravedad de las consecuencias de un incidente de ciberseguridad también puede acrecentarse dependiendo del uso previsto del producto***, como puede ocurrir*** en ***un entorno industrial*** o en el contexto de una entidad esencial contemplada en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como del desempeño de funciones críticas o sensibles, como el tratamiento de datos personales.	(25) Los productos con elementos digitales deben considerarse críticos si las consecuencias negativas del aprovechamiento de posibles vulnerabilidades de ciberseguridad en el producto pueden ser graves debido a, entre otras cosas, su funcionalidad relacionada con la ciberseguridad o su uso previsto. En particular, las vulnerabilidades de los productos con elementos digitales cuya funcionalidad está relacionada con la ciberseguridad, como los elementos seguros, pueden llevar a que los problemas de seguridad se propaguen a lo largo de la cadena de suministro. La gravedad de las consecuencias de un incidente de ciberseguridad también puede acrecentarse dependiendo del uso previsto del producto ***en aplicaciones críticas*** en ***entornos sensibles,*** o en el contexto de una entidad esencial contemplada en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)], así como del desempeño de funciones críticas o sensibles, como el tratamiento de datos personales.

Enmienda 16

Propuesta de Reglamento
Considerando 26

Texto de la Comisión	*Enmienda*
(26) Los productos críticos con elementos digitales deben estar sujetos a procedimientos de evaluación de la conformidad más estrictos, al tiempo que se garantiza un enfoque proporcionado. A tal fin, los productos críticos con elementos digitales deben dividirse en dos clases que reflejen el nivel de riesgo de	(26) Los productos críticos con elementos digitales deben estar sujetos a procedimientos de evaluación de la conformidad más estrictos, al tiempo que se garantiza un enfoque proporcionado. A tal fin, los productos críticos con elementos digitales deben dividirse en dos clases que reflejen el nivel de riesgo de

ciberseguridad presente en estas categorías de productos. Un posible incidente de ciberseguridad que afecte a productos de la clase II podría tener repercusiones negativas de mayor gravedad que un incidente que afecte a productos de la clase I, por ejemplo, debido a la naturaleza de su función vinculada a la ciberseguridad o su uso previsto en entornos sensibles, por lo que estos productos deben someterse a un procedimiento de evaluación de la conformidad más estricto.	ciberseguridad presente en estas categorías de productos. Un posible incidente de ciberseguridad que afecte a productos de la clase II podría tener repercusiones negativas de mayor gravedad que un incidente que afecte a productos de la clase I, por ejemplo, debido a la naturaleza de su función vinculada a la ciberseguridad o su uso previsto en entornos sensibles, por lo que estos productos deben someterse a un procedimiento de evaluación de la conformidad más estricto. ***Como excepción, las pequeñas empresas y las microempresas podrán utilizar el procedimiento para los productos de la clase I.***

Enmienda 17

Propuesta de Reglamento
Considerando 29

Texto de la Comisión	*Enmienda*
(29) Los productos con elementos digitales considerados sistemas de inteligencia artificial (IA) de alto riesgo con arreglo al artículo 6 del Reglamento [Reglamento sobre IA][27] que entren en el ámbito de aplicación del presente Reglamento deben cumplir los requisitos esenciales establecidos en el presente Reglamento**.** Cuando estos sistemas de IA de alto riesgo cumplan los requisitos esenciales del presente Reglamento, debe considerarse que cumplen los requisitos de ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA] en la medida en que dichos requisitos estén contemplados en la declaración UE de conformidad expedida en virtud del presente Reglamento o en partes de esta. Por lo que se refiere a los procedimientos de evaluación de la conformidad relativos a los requisitos esenciales de ciberseguridad de un producto con elementos digitales sujeto al presente Reglamento y considerado	(29) Los productos con elementos digitales ***o los productos parcialmente completados con elementos digitales*** considerados sistemas de inteligencia artificial (IA) de alto riesgo con arreglo al artículo 6 del Reglamento [Reglamento sobre IA][27] que entren en el ámbito de aplicación del presente Reglamento deben cumplir los requisitos esenciales establecidos en el presente Reglamento. Cuando estos sistemas de IA de alto riesgo cumplan los requisitos esenciales del presente Reglamento, debe considerarse que cumplen los requisitos de ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA] en la medida en que dichos requisitos estén contemplados en la declaración UE de conformidad expedida en virtud del presente Reglamento o en partes de esta. Por lo que se refiere a los procedimientos de evaluación de la conformidad relativos a los requisitos esenciales de ciberseguridad de un

sistema de IA de alto riesgo, las disposiciones pertinentes del ***artículo 43*** del Reglamento [Reglamento sobre IA] deben aplicarse como norma general en lugar de las respectivas disposiciones del presente Reglamento. ***Sin embargo,*** esta norma ***no*** debe ***dar lugar a una reducción del*** nivel de garantía ***necesario*** para los productos críticos con elementos digitales sujetos al presente Reglamento. ***Por consiguiente, no obstante lo dispuesto*** en ***esta norma,*** los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA], que asimismo se consideren productos críticos con elementos digitales con arreglo al presente Reglamento ***y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno especificado en*** el ***anexo VI del Reglamento [Reglamento sobre IA] deben estar sujetos*** a ***las disposiciones relativas a*** la evaluación de la conformidad ***incluidas en el*** presente Reglamento ***en la medida en que se refieran a los requisitos esenciales del presente Reglamento. En este caso, para todos*** los ***demás aspectos que entren en el ámbito*** de ***aplicación del Reglamento [Reglamento sobre IA], deben aplicarse las respectivas disposiciones relativas a la*** evaluación de la conformidad ***basadas en el control interno establecidas en el anexo VI del Reglamento [Reglamento sobre IA]***.	producto con elementos digitales sujeto al presente Reglamento y considerado sistema de IA de alto riesgo, las disposiciones pertinentes del ***[disposiciones aplicables]*** del Reglamento [Reglamento sobre IA] deben aplicarse como norma general en lugar de las respectivas disposiciones del presente Reglamento. Esta norma debe ***crear un elevado*** nivel de garantía para los productos críticos con elementos digitales sujetos al presente Reglamento. En ***el caso de*** los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA], que asimismo se consideren productos críticos con elementos digitales con arreglo al presente Reglamento***,*** el ***organismo notificado sectorial responsable debe encargarse de llevar*** a ***cabo*** la evaluación de la conformidad ***con arreglo al*** presente Reglamento***, y de dirigir el proceso administrativo de tal manera que*** los ***operadores económicos puedan dirigir su solicitud*** de evaluación de la conformidad ***a un único organismo regulador***.
[27] Reglamento [Reglamento sobre IA].	[27] Reglamento [Reglamento sobre IA].

Enmienda 18

Propuesta de Reglamento
Considerando 32

Texto de la Comisión	*Enmienda*
(32) Para garantizar que los productos con elementos digitales sean seguros tanto	(32) Para garantizar que los productos con elementos digitales sean seguros tanto

en el momento de su introducción en el mercado como a lo largo de su ciclo de vida, es necesario establecer requisitos esenciales para la gestión de las vulnerabilidades y requisitos esenciales de ciberseguridad relativos a las propiedades de los productos con elementos digitales. Si bien los fabricantes deben cumplir todos los requisitos esenciales en relación con la gestión de las vulnerabilidades y garantizar que todos sus productos se entreguen sin ninguna vulnerabilidad aprovechable conocida, también deben determinar qué otros requisitos esenciales relacionados con las propiedades del producto son pertinentes para el tipo de producto de que se trate. A tal fin, los fabricantes deben llevar a cabo una evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales para determinar los riesgos y los requisitos esenciales pertinentes y aplicar adecuadamente las normas armonizadas ***o especificaciones comunes*** apropiadas.	en el momento de su introducción en el mercado como a lo largo de su ciclo de vida, es necesario establecer requisitos esenciales para la gestión de las vulnerabilidades y requisitos esenciales de ciberseguridad relativos a las propiedades de los productos con elementos digitales. Si bien los fabricantes deben cumplir todos los requisitos esenciales en relación con la gestión de las vulnerabilidades y garantizar que todos sus productos se entreguen sin ninguna vulnerabilidad aprovechable conocida, también deben determinar qué otros requisitos esenciales relacionados con las propiedades del producto son pertinentes para el tipo de producto de que se trate. A tal fin, los fabricantes deben llevar a cabo una evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales para determinar los riesgos y los requisitos esenciales pertinentes y aplicar adecuadamente las normas armonizadas apropiadas.

Enmienda 19

Propuesta de Reglamento
Considerando 33 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(33 bis) Con el fin de garantizar que los productos se diseñen, desarrollen y fabriquen en consonancia con los requisitos esenciales previstos en la sección 1 del anexo I, los fabricantes deben ejercer la diligencia debida al integrar los componentes obtenidos de terceros en productos con elementos digitales. Esto ocurre con los componentes que se elaboran a medida y se integran teniendo en cuenta las especificidades del producto, en particular en el caso de los programas informáticos libres y de código abierto que no se hayan comercializado a cambio de una

monetización financiera o de otra índole.

Enmienda 20

Propuesta de Reglamento
Considerando 34

Texto de la Comisión	*Enmienda*
(34) Para garantizar que los CSIRT nacionales y los puntos de contacto únicos designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XX/XXXX (SRI 2)] reciban la información necesaria para desempeñar sus funciones y aumentar el nivel general de ciberseguridad de las entidades esenciales e importantes, así como para garantizar el funcionamiento efectivo de las autoridades de vigilancia del mercado, los fabricantes de productos con elementos digitales deben notificar a la ENISA las vulnerabilidades que se estén aprovechando activamente. Dado que la mayoría de los productos con elementos digitales se comercializan en todo el mercado interior, cualquier vulnerabilidad aprovechada en un producto con elementos digitales debe considerarse una amenaza para el funcionamiento del mercado interior. Los fabricantes también deben considerar la posibilidad de divulgar las vulnerabilidades subsanadas en la base de datos europea de vulnerabilidades creada en virtud de la Directiva [Directiva XX/XXXX (SRI 2)] y gestionada por la ENISA o en cualquier otra base de datos de vulnerabilidades que sea de acceso público.	(34) Para garantizar que los CSIRT nacionales y los puntos de contacto únicos designados de conformidad con el artículo [artículo X] de la Directiva [Directiva XX/XXXX (SRI 2)] reciban la información necesaria para desempeñar sus funciones y aumentar el nivel general de ciberseguridad de las entidades esenciales e importantes, así como para garantizar el funcionamiento efectivo de las autoridades de vigilancia del mercado, los fabricantes de productos con elementos digitales deben notificar a la ENISA***, sin demora indebida y, en cualquier caso, en un plazo de cuarenta y ocho horas a partir del momento en que tenga conocimiento de ello, mediante una alerta temprana*** las vulnerabilidades que se estén aprovechando activamente. ***Además, los fabricantes, sin demora indebida a partir del momento en que tengan conocimiento de una vulnerabilidad aprovechada que afecte de manera significativa a la seguridad del producto con elementos digitales, deben proporcionar a la ENISA información pormenorizada adicional sobre la vulnerabilidad de que se trate. Todas las demás vulnerabilidades que no afecten de manera significativa a la seguridad del producto con elementos digitales deben notificarse a la ENISA una vez que se haya abordado la vulnerabilidad.*** Dado que la mayoría de los productos con elementos digitales se comercializan en todo el mercado interior, cualquier vulnerabilidad aprovechada en un producto con elementos digitales debe considerarse una amenaza para el funcionamiento del mercado interior. Los fabricantes también

deben considerar la posibilidad de divulgar las vulnerabilidades subsanadas en la base de datos europea de vulnerabilidades creada en virtud de la Directiva [Directiva XX/XXXX (SRI 2)] y gestionada por la ENISA o en cualquier otra base de datos de vulnerabilidades que sea de acceso público.

Enmienda 21

Propuesta de Reglamento
Considerando 34 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(34 bis) La ENISA debe encargarse de publicar y mantener una base de datos de vulnerabilidades aprovechadas conocidas. Los fabricantes deben llevar a cabo un seguimiento de dicha base y notificar las vulnerabilidades encontradas en sus productos.

Enmienda 22

Propuesta de Reglamento
Considerando 35

Texto de la Comisión	*Enmienda*
(35) Los fabricantes también deben notificar a la ENISA cualquier incidente que repercuta en la seguridad del producto con elementos digitales. Sin perjuicio de las obligaciones de notificación de incidentes establecidas en la Directiva [Directiva XXX/XXXX (SRI 2)] para las entidades esenciales e importantes, es fundamental que los fabricantes de productos con elementos digitales proporcionen a la ENISA, a los puntos de contacto únicos designados por los Estados miembros de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] y a las autoridades de vigilancia del mercado información que	(35) Los fabricantes también deben notificar a la ENISA***, mediante una alerta temprana,*** cualquier incidente que repercuta ***significativamente*** en la seguridad del producto con elementos digitales. ***Los fabricantes proporcionarán a la ENISA, sin demora indebida, y en cualquier caso en un plazo de setenta y dos horas a partir del momento en que tengan conocimiento del incidente significativo relacionado con el producto con elementos digitales, información pormenorizada adicional sobre el incidente significativo de que se trate.*** Sin perjuicio de las obligaciones de notificación de incidentes establecidas en

les permita evaluar la seguridad de dichos productos. Para garantizar que los usuarios puedan reaccionar rápidamente ante incidentes que repercutan en la seguridad de sus productos con elementos digitales, los fabricantes también deben informar a sus usuarios sobre cualquier incidente de este tipo y, en su caso, sobre las medidas correctoras que los usuarios puedan adoptar para mitigar las repercusiones del incidente, por ejemplo, mediante la publicación de la información pertinente en sus sitios web o, cuando el fabricante pueda ponerse en contacto con los usuarios y los riesgos lo justifiquen, comunicándose directamente con ellos.	la Directiva [Directiva XXX/XXXX (SRI 2)] para las entidades esenciales e importantes, es fundamental que los fabricantes de productos con elementos digitales proporcionen a la ENISA, a los puntos de contacto únicos designados por los Estados miembros de conformidad con el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] y a las autoridades de vigilancia del mercado información que les permita evaluar la seguridad de dichos productos. Para garantizar que los usuarios puedan reaccionar rápidamente ante incidentes que repercutan ***de manera significativa*** en la seguridad de sus productos con elementos digitales, los fabricantes también deben informar a sus usuarios***, cuando proceda y si es probable que este les afecte negativamente,*** sobre cualquier incidente de este tipo y, en su caso, sobre las medidas ***de mitigación de riesgos y*** correctoras que los usuarios puedan adoptar para mitigar las repercusiones del incidente ***significativo***, por ejemplo, mediante la publicación de la información pertinente en sus sitios web o, cuando el fabricante pueda ponerse en contacto con los usuarios y los riesgos lo justifiquen, comunicándose directamente con ellos. ***Sin perjuicio del resto de sus obligaciones, los fabricantes que detecten una vulnerabilidad en un componente integrado en un producto con elementos digitales, y en particular, en un componente libre y de código abierto, deben notificar la vulnerabilidad a la persona física o jurídica que mantenga el componente, junto con las medidas correctivas adoptadas.***

Enmienda 23

Propuesta de Reglamento
Considerando 37 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(37 bis) En virtud del Acuerdo sobre Obstáculos Técnicos al Comercio de la OMC, cuando se precisen reglamentos técnicos y existan normas internacionales pertinentes, los miembros de la OMC deben utilizar dichas normas como base para la elaboración de sus propios reglamentos técnicos. Es importante evitar la duplicación de tareas entre las organizaciones de normalización, habida cuenta de que con las normas internacionales se pretende facilitar la armonización de los reglamentos y las normas técnicos nacionales y regionales, reduciendo de este modo las barreras técnicas no arancelarias al comercio. Dado que la ciberseguridad es un asunto de alcance mundial, la Unión debe esforzarse por procurar la máxima coherencia. A tal efecto, la solicitud de normalización respecto al presente Reglamento, conforme se dispone en el artículo 10 del Reglamento (UE) n.º 1025/2012, debe perseguir que se reduzcan las barreras a la aceptación de normas mediante la publicación de sus referencias en el Diario Oficial de la UE, de conformidad con el artículo 10, apartado 6, del Reglamento (UE) n.º 1025/2012.

Enmienda 24

Propuesta de Reglamento
Considerando 37 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(37 ter) Habida cuenta del amplio alcance del presente Reglamento, el desarrollo oportuno de normas armonizadas plantea un reto significativo. Con el fin de reforzar la seguridad de los productos con componentes digitales en el mercado de la Unión a la mayor brevedad

posible, la Comisión debe estar facultada, durante un período limitado, para declarar que las normas internacionales sobre ciberseguridad de los productos satisfacen los requisitos del presente Reglamento. Deberán publicarse como normas que proporcionan presunción de conformidad.

Enmienda 25

Propuesta de Reglamento
Considerando 38

Texto de la Comisión	*Enmienda*
(38) A fin de facilitar la evaluación de la conformidad con los requisitos establecidos en el presente Reglamento, debe aplicarse una presunción de conformidad de los productos con elementos digitales que sean conformes con normas armonizadas que plasmen los requisitos esenciales del presente Reglamento en especificaciones técnicas detalladas y se adopten con arreglo al Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[29]. El Reglamento (UE) n.º 1025/2012 establece un procedimiento de presentación de objeciones a las normas armonizadas para el caso en que estas no cumplan plenamente los requisitos del presente Reglamento.	(38) A fin de facilitar la evaluación de la conformidad con los requisitos establecidos en el presente Reglamento, debe aplicarse una presunción de conformidad de los productos con elementos digitales que sean conformes con normas armonizadas que plasmen los requisitos esenciales del presente Reglamento en especificaciones técnicas detalladas y se adopten con arreglo al Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[29]. El Reglamento (UE) n.º 1025/2012 establece un procedimiento de presentación de objeciones a las normas armonizadas para el caso en que estas no cumplan plenamente los requisitos del presente Reglamento. ***El proceso de normalización debe garantizar una representación equilibrada de intereses y la participación efectiva de las partes interesadas de la sociedad civil, incluidas las organizaciones de consumidores.***
[29] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE,	[29] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE,

2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

Enmienda 26

Propuesta de Reglamento
Considerando 41

Texto de la Comisión	*Enmienda*
(41) Cuando no se ***adopten normas armonizadas o cuando las*** normas armonizadas ***no tengan suficientemente*** en ***cuenta los requisitos esenciales del presente*** Reglamento, la Comisión debe poder adoptar especificaciones comunes mediante actos de ejecución. Las razones para elaborar estas especificaciones comunes en lugar de basarse en normas armonizadas pueden incluir la denegación de la solicitud de normalización por parte de cualquiera de los organismos europeos de normalización, retrasos indebidos en el establecimiento de normas armonizadas apropiadas o la falta de conformidad de las normas establecidas con los requisitos del presente Reglamento o con una petición de la Comisión. Para facilitar la evaluación de la conformidad con los requisitos esenciales establecidos en el presente Reglamento, debe presuponerse la conformidad de los productos con elementos digitales que sean conformes con las especificaciones comunes adoptadas por la Comisión con arreglo al presente Reglamento a fin de indicar las especificaciones técnicas detalladas de dichos requisitos.	(41) Cuando no se ***haya publicado en el Diario Oficial de la Unión Europea ninguna referencia a*** normas armonizadas ***que regulen los requisitos establecidos*** en ***el anexo I de conformidad con el*** Reglamento ***(UE) n.º 1025/2012 y no se prevea la publicación de ninguna referencia de este tipo en un plazo razonable***, la Comisión debe poder adoptar especificaciones comunes mediante actos de ejecución. Las razones para elaborar estas especificaciones comunes en lugar de basarse en normas armonizadas pueden incluir la denegación de la solicitud de normalización por parte de cualquiera de los organismos europeos de normalización, retrasos indebidos en el establecimiento de normas armonizadas apropiadas o la falta de conformidad de las normas establecidas con los requisitos del presente Reglamento o con una petición de la Comisión. Para facilitar la evaluación de la conformidad con los requisitos esenciales establecidos en el presente Reglamento, debe presuponerse la conformidad de los productos con elementos digitales que sean conformes con las especificaciones comunes adoptadas por la Comisión con arreglo al presente Reglamento a fin de indicar las especificaciones técnicas detalladas de dichos requisitos.

Enmienda 27

Propuesta de Reglamento
Considerando 43

Texto de la Comisión	*Enmienda*
(43) El marcado CE, que indica la conformidad de un producto, es el resultado visible de todo un proceso que comprende la evaluación de la conformidad en sentido amplio. Los principios generales por los que se rige el marcado CE se establecen en el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo[30]. En el presente Reglamento deben establecerse normas relativas a la colocación del marcado CE en productos con elementos digitales. El marcado CE debe ser el único marcado que garantice que los productos con elementos digitales cumplen con los requisitos del presente Reglamento.	(43) El marcado CE, que indica la conformidad de un producto, es el resultado visible de todo un proceso que comprende la evaluación de la conformidad en sentido amplio. Los principios generales por los que se rige el marcado CE se establecen en el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo[30]. En el presente Reglamento deben establecerse normas relativas a la colocación del marcado CE en productos con elementos digitales. El marcado CE debe ser el único marcado que garantice que los productos con elementos digitales cumplen con los requisitos del presente Reglamento. ***Sin embargo, un producto parcialmente completado con elementos digitales no se marcará con el marcado CE conforme al presente Reglamento, sin perjuicio de las disposiciones sobre marcado que se deriven de otra legislación aplicable de la Unión. Para los productos parcialmente completados con elementos digitales, los fabricantes deben elaborar una declaración UE de incorporación.***
[30] 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 por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).	[30] 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 por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

Enmienda 28

Propuesta de Reglamento
Considerando 45

Texto de la Comisión	*Enmienda*
(45) Como norma general, ***el fabricante debe llevar a cabo*** la evaluación de la conformidad de los productos con elementos digitales bajo su propia responsabilidad mediante un procedimiento basado en el módulo A de la Decisión n.º 768/2008/CE. El fabricante deberá ser flexible en lo que se refiere a la elección de un procedimiento de evaluación de la conformidad más estricto en el que participe un tercero. Si el producto está considerado producto crítico de la clase I, se requieren garantías adicionales para demostrar la conformidad con los requisitos esenciales establecidos en el presente Reglamento. Si el fabricante desea llevar a cabo la evaluación de la conformidad bajo su propia responsabilidad (módulo A), debe aplicar normas armonizadas***, especificaciones comunes*** o esquemas de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 que hayan sido reconocidos por la Comisión mediante acto de ejecución. Si el fabricante no aplica estas normas armonizadas***, especificaciones comunes*** o esquemas de certificación de la ciberseguridad, debe someterse a una evaluación de la conformidad en la que participe un tercero. Teniendo en cuenta la carga administrativa de los fabricantes y el hecho de que la ciberseguridad desempeña un papel importante en la fase de diseño y desarrollo de productos tangibles e intangibles con elementos digitales, los procedimientos de evaluación de la conformidad basados, respectivamente, en los módulos B + C o H de la Decisión n.º 768/2008/CE han sido elegidos como los más adecuados para evaluar la conformidad de los productos críticos con los elementos digitales de manera proporcionada y eficaz. El fabricante que opte por la evaluación de la conformidad de terceros puede elegir el procedimiento que mejor se adapte a su proceso de diseño	(45) Como norma general, ***los requisitos de*** la evaluación de la conformidad de los productos con elementos digitales ***deben basarse en el riesgo y, en ese sentido, en muchos casos, el fabricante podría llevar a cabo tal evaluación*** bajo su propia responsabilidad mediante un procedimiento basado en el módulo A de la Decisión n.º 768/2008/CE. El fabricante deberá ser flexible en lo que se refiere a la elección de un procedimiento de evaluación de la conformidad más estricto en el que participe un tercero. Si el producto está considerado producto crítico de la clase I, se requieren garantías adicionales para demostrar la conformidad con los requisitos esenciales establecidos en el presente Reglamento. Si el fabricante desea llevar a cabo la evaluación de la conformidad bajo su propia responsabilidad (módulo A), debe aplicar normas armonizadas o esquemas de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 que hayan sido reconocidos por la Comisión mediante ***un*** acto de ejecución. Si el fabricante no aplica estas normas armonizadas o esquemas de certificación de la ciberseguridad, debe someterse a una evaluación de la conformidad en la que participe un tercero. Teniendo en cuenta la carga administrativa de los fabricantes y el hecho de que la ciberseguridad desempeña un papel importante en la fase de diseño y desarrollo de productos tangibles e intangibles con elementos digitales, los procedimientos de evaluación de la conformidad basados, respectivamente, en los módulos B + C o H de la Decisión n.º 768/2008/CE han sido elegidos como los más adecuados para evaluar la conformidad de los productos críticos con los elementos digitales de manera proporcionada y eficaz. El fabricante que opte por la evaluación de la conformidad de terceros puede elegir el procedimiento

y producción. Habida cuenta del riesgo de ciberseguridad aún mayor asociado al uso de productos clasificados como productos críticos de la clase II, la evaluación de la conformidad de estos productos siempre debe contar con la participación de un tercero.	que mejor se adapte a su proceso de diseño y producción. Habida cuenta del riesgo de ciberseguridad aún mayor asociado al uso de productos clasificados como productos críticos de la clase II, la evaluación de la conformidad de estos productos siempre debe contar con la participación de un tercero.

Enmienda 29

Propuesta de Reglamento
Considerando 46 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(46 bis) Cuando los productos con elementos digitales sean equivalentes, uno de estos productos puede aceptarse como representativo de una familia o categoría de productos a efectos de determinados procedimientos de evaluación de la conformidad.

Enmienda 30

Propuesta de Reglamento
Considerando 55

Texto de la Comisión	*Enmienda*
(55) De conformidad con el Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado son responsables de efectuar la vigilancia del mercado en el territorio del Estado miembro correspondiente. El presente Reglamento no debe impedir que los Estados miembros escojan a las autoridades competentes que desempeñan esas tareas. Cada Estado miembro debe designar a una o varias autoridades de vigilancia del mercado en su territorio. Los Estados miembros podrán optar por designar a cualquier autoridad existente o nueva para que actúe en calidad de autoridad de vigilancia del mercado,	(55) De conformidad con el Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado son responsables de efectuar la vigilancia del mercado en el territorio del Estado miembro correspondiente. El presente Reglamento no debe impedir que los Estados miembros escojan a las autoridades competentes que desempeñan esas tareas. Cada Estado miembro debe designar a una o varias autoridades de vigilancia del mercado en su territorio. Los Estados miembros podrán optar por designar a cualquier autoridad existente o nueva para que actúe en calidad de autoridad de vigilancia del mercado,

incluidas las autoridades nacionales competentes especificadas en el artículo ***[artículo X]*** de la Directiva ***[Directiva XXX/XXXX*** (SRI 2)***] y*** las autoridades nacionales de certificación de la ciberseguridad designadas a las que hace referencia el artículo 58 del Reglamento (UE) 2019/881. Los operadores económicos deben cooperar plenamente con las autoridades de vigilancia del mercado y otras autoridades competentes. Cada Estado miembro debe informar a la Comisión y a los demás Estados miembros acerca de sus autoridades de vigilancia del mercado y de los ámbitos de competencia de cada una de ellas, así como garantizar las capacidades y los recursos necesarios para desempeñar las funciones de vigilancia relacionadas con el presente Reglamento. De conformidad con el artículo 10, apartados 2 y 3, del Reglamento (UE) 2019/1020, cada Estado miembro debe designar una oficina de enlace única que debe ser responsable de, entre otras cosas, representar la posición coordinada de las autoridades de vigilancia del mercado y prestar asistencia en la cooperación entre las autoridades de vigilancia del mercado en diferentes Estados miembros.	incluidas las autoridades nacionales competentes especificadas en el artículo ***8*** de la 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) ***o*** las autoridades nacionales de certificación de la ciberseguridad designadas a las que hace referencia el artículo 58 del Reglamento (UE) 2019/881. Los operadores económicos deben cooperar plenamente con las autoridades de vigilancia del mercado y otras autoridades competentes. Cada Estado miembro debe informar a la Comisión y a los demás Estados miembros acerca de sus autoridades de vigilancia del mercado y de los ámbitos de competencia de cada una de ellas, así como garantizar las capacidades y los recursos necesarios para desempeñar las funciones de vigilancia relacionadas con el presente Reglamento. De conformidad con el artículo 10, apartados 2 y 3, del Reglamento (UE) 2019/1020, cada Estado miembro debe designar una oficina de enlace única que debe ser responsable de, entre otras cosas, representar la posición coordinada de las autoridades de vigilancia del mercado y prestar asistencia en la cooperación entre las autoridades de vigilancia del mercado en diferentes Estados miembros.

Enmienda 31

Propuesta de Reglamento
Considerando 56 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(56 bis) A fin de que los operadores económicos que sean pymes y

microempresas puedan hacer frente a las nuevas obligaciones impuestas por el presente Reglamento, la Comisión debe facilitarles directrices y asesoramiento fáciles de entender, por ejemplo, a través de un canal directo para contactar con expertos en caso de que tengan preguntas, teniendo en cuenta la necesidad de simplificar y limitar las cargas administrativas. Al elaborar dichas directrices, la Comisión debe tener en cuenta las necesidades de las pymes de modo que se reduzcan al mínimo las cargas administrativas y financieras, facilitando al mismo tiempo su cumplimiento del presente Reglamento. La Comisión debe consultar a las partes interesadas pertinentes con conocimientos técnicos en el ámbito de la ciberseguridad.

Enmienda 32

Propuesta de Reglamento
Considerando 58

Texto de la Comisión	*Enmienda*
(58) En determinados casos, un producto con elementos digitales que cumpla lo dispuesto en el presente Reglamento puede, no obstante, presentar un riesgo de ciberseguridad significativo o plantear un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones en virtud del Derecho nacional o de la Unión en materia de protección de los derechos fundamentales, para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema de información electrónico por entidades esenciales contempladas en el ***[***anexo I de la Directiva ***XXX/XXXX*** (SRI 2)***]*** o para otros aspectos relativos a la protección del interés público. Es por tanto necesario establecer normas que garanticen la mitigación de estos riesgos. En consecuencia, las autoridades de vigilancia	(58) En determinados casos, un producto con elementos digitales que cumpla lo dispuesto en el presente Reglamento puede, no obstante, presentar un riesgo de ciberseguridad significativo o plantear un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones en virtud del Derecho nacional o de la Unión en materia de protección de los derechos fundamentales, para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema de información electrónico por entidades esenciales contempladas en el anexo I de la Directiva ***(UE) 2022/2555*** (SRI 2) o para otros aspectos relativos a la protección del interés público. Es por tanto necesario establecer normas que garanticen la mitigación de estos riesgos. En consecuencia, las autoridades de vigilancia

del mercado deben adoptar medidas para exigir al operador económico que se asegure de que el producto ya no presente dicho riesgo, retirarlo del mercado o recuperarlo, dependiendo del riesgo que presente. Tan pronto como una autoridad de vigilancia del mercado restrinja o prohíba la libre circulación de un producto de esa manera, el Estado miembro debe notificar inmediatamente a la Comisión y a los demás Estados miembros las medidas provisionales, indicando las razones y la justificación de esa decisión. Cuando una autoridad de vigilancia del mercado adopte tales medidas contra productos que planteen un riesgo, la Comisión debe consultar sin demora a los Estados miembros y al operador o los operadores económicos pertinentes y debe evaluar la medida nacional. Basándose en los resultados de dicha evaluación, la Comisión debe decidir si la medida nacional está o no justificada. La Comisión debe comunicar inmediatamente su decisión a todos los Estados miembros y al operador o los operadores económicos pertinentes. Si la medida se considera justificada, la Comisión también puede considerar la adopción de propuestas para revisar la legislación de la Unión que corresponda.

del mercado deben adoptar medidas para exigir al operador económico que se asegure de que el producto ya no presente dicho riesgo, retirarlo del mercado o recuperarlo, dependiendo del riesgo que presente. Tan pronto como una autoridad de vigilancia del mercado restrinja o prohíba la libre circulación de un producto de esa manera, el Estado miembro debe notificar inmediatamente a la Comisión y a los demás Estados miembros las medidas provisionales, indicando las razones y la justificación de esa decisión. Cuando una autoridad de vigilancia del mercado adopte tales medidas contra productos que planteen un riesgo, la Comisión debe consultar sin demora a los Estados miembros y al operador o los operadores económicos pertinentes y debe evaluar la medida nacional. Basándose en los resultados de dicha evaluación, la Comisión debe decidir si la medida nacional está o no justificada. La Comisión debe comunicar inmediatamente su decisión a todos los Estados miembros y al operador o los operadores económicos pertinentes. Si la medida se considera justificada, la Comisión también puede considerar la adopción de propuestas para revisar la legislación de la Unión que corresponda.

Enmienda 33

Propuesta de Reglamento
Considerando 59

Texto de la Comisión	*Enmienda*
(59) Por lo que respecta a los productos con elementos digitales que presenten un riesgo de ciberseguridad significativo y en relación con los cuales existan motivos para creer que no son conformes con el presente Reglamento, o bien a los productos que son conformes con el presente Reglamento pero presentan otros riesgos importantes, como riesgos para la	(59) Por lo que respecta a los productos con elementos digitales que presenten un riesgo de ciberseguridad significativo y en relación con los cuales existan motivos para creer que no son conformes con el presente Reglamento, o bien a los productos que son conformes con el presente Reglamento pero presentan otros riesgos importantes, como riesgos para la

salud o la seguridad de las personas, los derechos fundamentales o la prestación de servicios por parte de entidades esenciales del tipo contemplado en el ***[***anexo I de la Directiva ***XXX/XXXX*** (SRI 2)***]***, la Comisión podrá solicitar a la ENISA que lleve a cabo una evaluación. Sobre la base de dicha evaluación, la Comisión podrá adoptar, mediante actos de ejecución, medidas correctoras o restrictivas a escala de la Unión, como retirar del mercado o recuperar los productos correspondientes en un plazo razonable, proporcional a la naturaleza del riesgo. La Comisión solo puede recurrir a tal medida en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y únicamente cuando las autoridades de vigilancia no hayan adoptado medidas eficaces para remediar la situación. Estas circunstancias excepcionales pueden darse en situaciones de emergencia en las que, por ejemplo, un fabricante comercialice de manera generalizada en varios Estados miembros un producto no conforme utilizado asimismo en sectores clave por entidades incluidas en el ámbito de aplicación de la ***[***Directiva ***XXX/XXXX*** (SRI 2)***]***, a pesar de contener vulnerabilidades conocidas que estén siendo aprovechadas por agentes malintencionados y para las que el fabricante no proporcione parches disponibles. La Comisión solo podrá intervenir en situaciones de emergencia de este tipo mientras duren las circunstancias excepcionales y si persiste el incumplimiento del presente Reglamento o los riesgos importantes detectados.

salud o la seguridad de las personas, los derechos fundamentales o la prestación de servicios por parte de entidades esenciales del tipo contemplado en el anexo I de la Directiva ***(UE) 2022/2555*** (SRI 2), la Comisión podrá solicitar a la ENISA que lleve a cabo una evaluación. Sobre la base de dicha evaluación, la Comisión podrá adoptar, mediante actos de ejecución, medidas correctoras o restrictivas a escala de la Unión, como retirar del mercado o recuperar los productos correspondientes en un plazo razonable, proporcional a la naturaleza del riesgo. La Comisión solo puede recurrir a tal medida en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y únicamente cuando las autoridades de vigilancia no hayan adoptado medidas eficaces para remediar la situación. Estas circunstancias excepcionales pueden darse en situaciones de emergencia en las que, por ejemplo, un fabricante comercialice de manera generalizada en varios Estados miembros un producto no conforme utilizado asimismo en sectores clave por entidades incluidas en el ámbito de aplicación de la Directiva ***(UE) 2022/2555*** (SRI 2), a pesar de contener vulnerabilidades conocidas que estén siendo aprovechadas por agentes malintencionados y para las que el fabricante no proporcione parches disponibles. La Comisión solo podrá intervenir en situaciones de emergencia de este tipo mientras duren las circunstancias excepcionales y si persiste el incumplimiento del presente Reglamento o los riesgos importantes detectados.

Enmienda 34

Propuesta de Reglamento
Considerando 62

Texto de la Comisión	*Enmienda*
(62) A fin de garantizar que el marco regulador pueda adaptarse cuando sea necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo a lo dispuesto en el artículo 290 del Tratado a efectos de actualizar la lista de productos críticos del anexo III y especificar las definiciones de dichas categorías de productos. Deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo a fin de identificar los productos con elementos digitales regulados por otras normas de la Unión que alcancen el mismo nivel de protección que el presente Reglamento, especificando si sería necesaria una limitación o una exclusión del ámbito de aplicación del presente Reglamento, así como, en su caso, el alcance de dicha limitación. También deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo con respecto a la posible ***exigencia de*** certificación de determinados productos altamente críticos con elementos digitales, sobre la base de criterios de criticidad establecidos en el presente Reglamento, así como con respecto a la especificación del contenido mínimo de la declaración UE de conformidad y al complemento de los elementos que deban incluirse en la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional sobre la Mejora de la Legislación, de 13 de abril de 2016[33]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus	(62) A fin de garantizar que el marco regulador pueda adaptarse cuando sea necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo a lo dispuesto en el artículo 290 del Tratado a efectos de actualizar la lista de productos críticos del anexo III y especificar las definiciones de dichas categorías de productos. Deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo a fin de identificar los productos con elementos digitales regulados por otras normas de la Unión que alcancen el mismo nivel de protección que el presente Reglamento, especificando si sería necesaria una limitación o una exclusión del ámbito de aplicación del presente Reglamento, así como, en su caso, el alcance de dicha limitación. También deben delegarse en la Comisión los poderes para adoptar actos con arreglo a dicho artículo con respecto a la posible certificación ***voluntaria*** de determinados productos altamente críticos con elementos digitales, sobre la base de criterios de criticidad establecidos en el presente Reglamento, así como con respecto a la especificación del contenido mínimo de la declaración UE de conformidad y al complemento de los elementos que deban incluirse en la documentación técnica. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional sobre la Mejora de la Legislación, de 13 de abril de 2016[33]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus

expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

[33] DO L 123 de 12.5.2016, p. 1.

expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

[33] DO L 123 de 12.5.2016, p. 1.

Enmienda 35

Propuesta de Reglamento
Considerando 63

Texto de la Comisión	*Enmienda*
(63) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para: especificar el formato y los elementos de la nomenclatura de materiales de los programas informáticos; especificar el tipo de información, el formato y el procedimiento para las notificaciones de vulnerabilidades aprovechadas activamente e incidentes presentadas por los fabricantes a la ENISA; especificar los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que puedan utilizarse para demostrar la conformidad con los requisitos esenciales, o partes de estos, establecidos en el anexo I del presente Reglamento; adoptar especificaciones comunes relacionadas con los requisitos esenciales establecidos en el anexo I; establecer especificaciones técnicas para los pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales y mecanismos para promover su uso; y adoptar decisiones sobre medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior. Dichas competencias deben ejercerse de conformidad con el	(63) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para: especificar el formato y los elementos de la nomenclatura de materiales de los programas informáticos; especificar el tipo de información, el formato y el procedimiento para las notificaciones de vulnerabilidades aprovechadas activamente e incidentes presentadas por los fabricantes a la ENISA***, sobre la base de las mejores prácticas sectoriales***; especificar los esquemas europeos de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 que puedan utilizarse para demostrar la conformidad con los requisitos esenciales, o partes de estos, establecidos en el anexo I del presente Reglamento; adoptar especificaciones comunes relacionadas con los requisitos esenciales establecidos en el anexo I; establecer especificaciones técnicas para los pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales y mecanismos para promover su uso; y adoptar decisiones sobre medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior. Dichas competencias

Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[34].	deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[34].
[34] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).	[34] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

Enmienda 36

Propuesta de Reglamento
Considerando 69

Texto de la Comisión	*Enmienda*
(69) Los operadores económicos deben disponer de tiempo suficiente para adaptarse a los requisitos del presente Reglamento. El presente Reglamento debe ser aplicable [***veinticuatro*** meses] después de su entrada en vigor***, a excepción de las obligaciones de información relativas a vulnerabilidades aprovechadas activamente e incidentes, que deben ser aplicables [doce meses] después de la entrada en vigor del presente Reglamento***.	(69) Los operadores económicos deben disponer de tiempo suficiente para adaptarse a los requisitos del presente Reglamento. El presente Reglamento debe ser aplicable [***treinta y seis*** meses] después de su entrada en vigor.

Enmienda 37

Propuesta de Reglamento
Artículo 1 – párrafo 1 – parte introductoria

Texto de la Comisión	*Enmienda*
El presente Reglamento establece:	***El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior, garantizando al mismo tiempo un nivel elevado de protección de los consumidores y de ciberseguridad.***

	El presente Reglamento establece ***disposiciones armonizadas sobre***:

Enmienda 38

Propuesta de Reglamento
Artículo 1 – párrafo 1 – letra a

Texto de la Comisión	*Enmienda*
a) ***normas para*** la introducción en el mercado de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos;	a) la introducción en el mercado de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos;

Enmienda 39

Propuesta de Reglamento
Artículo 1 – párrafo 1 – letra d

Texto de la Comisión	*Enmienda*
d) ***normas relativas a*** la vigilancia del mercado y ***a*** la aplicación de los requisitos y las normas antes mencionados.	d) la vigilancia del mercado y la aplicación de los requisitos y las normas antes mencionados.

Enmienda 40

Propuesta de Reglamento
Artículo 2 – apartado 1

Texto de la Comisión	*Enmienda*
1. El presente Reglamento es aplicable a los productos con elementos digitales cuyo uso previsto o razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.	1. El presente Reglamento es aplicable a los productos con elementos digitales ***comercializados*** cuyo uso previsto o razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red ***externos***.

Enmienda 41

Propuesta de Reglamento
Artículo 2 – apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. El presente Reglamento no se aplica a los programas informáticos libres y de código abierto, incluido su código fuente y las versiones modificadas, excepto cuando dicho programa informático se proporcione a cambio de una actividad comercial, ya sea:
	i) por la aplicación de un precio a un producto;
	ii) suministrando una plataforma de software que se sirva de otros servicios que el fabricante monetiza;
	iii) utilizando datos personales generados por el programa informático por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático;
	iv) aplicando un precio a los servicios de asistencia técnica.
	El fabricante se encargará de garantizar la conformidad de los componentes libres y de código abierto de los productos en los que estén incluidos.

Enmienda 42

Propuesta de Reglamento
Artículo 2 – apartado 5 ter (nuevo)

Texto de la Comisión	*Enmienda*
	5 ter. El presente Reglamento no se aplica a las redes internas de un producto con elementos digitales si tales redes disponen de nodos finales dedicados y están protegidas frente a las conexiones de datos externas.

Enmienda 43

Propuesta de Reglamento
Artículo 2 – apartado 5 quater (nuevo)

Texto de la Comisión	*Enmienda*
	5 quater. El presente Reglamento no se aplicará a las piezas de repuesto destinadas únicamente a sustituir piezas defectuosas de productos con elementos digitales con el fin de restablecer su funcionalidad.

Enmienda 44

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 1

Texto de la Comisión	*Enmienda*
1) «producto con elementos digitales»: cualquier producto consistente en programas informáticos o equipos informáticos ***y sus soluciones de tratamiento de datos a distancia***, incluidos los componentes de programas informáticos o equipos informáticos que se introduzcan en el mercado por separado;	1) «producto con elementos digitales»: cualquier producto consistente en programas informáticos o equipos informáticos, incluidos los componentes de programas informáticos o equipos informáticos que se introduzcan en el mercado por separado;

Enmienda 45

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
2) «tratamiento de datos a distancia»: todo tratamiento de datos a distancia para el que el programa informático ha sido diseñado y desarrollado por el fabricante del producto en cuestión o bajo su responsabilidad, y cuya ausencia impediría que el producto con elementos digitales cumpliera alguna de sus funciones;	***suprimido***

Enmienda 46

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	6 bis) «programa informático de código abierto»: programa informático distribuido bajo licencia que permite a los usuarios proceder libremente a su ejecución, copia, distribución, estudio, modificación o mejora, así como a su integración como componente en otros productos, su prestación como servicio, o a la prestación de apoyo comercial para el mismo;

Enmienda 47

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 18

Texto de la Comisión	*Enmienda*
18) «fabricante»: toda persona física o jurídica que desarrolla o fabrica productos con elementos digitales o para quien se diseñan, desarrollan o fabrican productos con elementos digitales, y que los comercializa con su nombre o marca comercial, ya sea de manera remunerada o gratuita;	*(No afecta a la versión española).*

Enmienda 48

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 19

Texto de la Comisión	*Enmienda*
19) «representante autorizado»: toda persona física o jurídica establecida en la Unión que ha recibido un mandato escrito de un fabricante para actuar en su nombre	19) «representante autorizado»: toda persona física o jurídica establecida en la Unión que ha recibido un mandato escrito de un fabricante para actuar en su nombre

en relación con tareas especificadas;	en relación con tareas especificadas ***relativas a las obligaciones del fabricante***;

Enmienda 49

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 23 bis (nuevo)

Texto de la Comisión	*Enmienda*
	23 bis) «recuperación»: la recuperación según se define en el artículo 3, punto 22, del Reglamento (UE) 2019/1020;

Enmienda 50

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 26

Texto de la Comisión	*Enmienda*
26) «uso indebido razonablemente previsible»: el uso de un producto con elementos digitales de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas razonablemente previsible;	***suprimido***

Enmienda 51

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 31

Texto de la Comisión	*Enmienda*
31) «modificación sustancial»: un cambio en un producto con elementos digitales tras su introducción en el mercado que afecta al cumplimiento por parte del producto de los requisitos esenciales establecidos en la sección 1 del anexo I o que provoca la modificación de la finalidad prevista para la que se ha evaluado el	31) «modificación sustancial»: un cambio en un producto con elementos digitales***, con exclusión de las actualizaciones de seguridad y de mantenimiento,*** tras su introducción en el mercado que afecta al cumplimiento por parte del producto de los requisitos esenciales establecidos en la sección 1 del

producto con elementos digitales;	anexo I o que provoca la modificación de la finalidad prevista para la que se ha evaluado el producto con elementos digitales;

Enmienda 52

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 39

Texto de la Comisión	*Enmienda*
39) «vulnerabilidad aprovechada activamente»: una vulnerabilidad respecto de la cual existen pruebas fiables de la ejecución de un código malicioso en un sistema por parte de un agente sin autorización del propietario del sistema;	39) «vulnerabilidad aprovechada activamente»: una vulnerabilidad ***parcheada*** respecto de la cual existen pruebas fiables de la ejecución de un código malicioso en un sistema por parte de un agente sin autorización del propietario del sistema;

Enmienda 53

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 40 bis (nuevo)

Texto de la Comisión	*Enmienda*
	40 bis) «productos parcialmente completados con elementos digitales»: un producto tangible que no puede funcionar de manera independiente y que solo se produce con el objetivo de su incorporación o su montaje en un producto con elementos digitales u otro producto parcialmente completado con elementos digitales, y cuya conformidad solo puede evaluarse eficazmente teniendo en cuenta el modo en que se incorpora a un producto con elementos digitales concebido como definitivo;

Enmienda 54

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 40 ter (nuevo)

Texto de la Comisión	*Enmienda*
	40 ter) «vida útil»: período comprendido entre el momento en que un producto cubierto por el presente Reglamento se introduce en el mercado o se pone en servicio y el momento en que es descartado, lo que incluye el tiempo efectivo en que puede utilizarse y las etapas de transporte, montaje, desmontaje, desactivación, desguace u otras modificaciones físicas o digitales previstas por el fabricante.

Enmienda 55

Propuesta de Reglamento
Artículo 4 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros no impedirán, por los aspectos contemplados en el presente Reglamento, la comercialización de productos con elementos digitales que sean conformes con el presente Reglamento.	1. Los Estados miembros no impedirán, por los aspectos contemplados en el presente Reglamento, la comercialización de productos con elementos digitales ***o de productos parcialmente completados con elementos digitales*** que sean conformes con el presente Reglamento.

Enmienda 56

Propuesta de Reglamento
Artículo 4 – apartado 2

Texto de la Comisión	*Enmienda*
2. Los Estados miembros no impedirán que en ferias, exposiciones, demostraciones o actos similares se presenten y usen productos con elementos digitales que no sean conformes con el presente Reglamento.	2. Los Estados miembros no impedirán que en ferias, exposiciones, demostraciones o actos similares se presenten y usen productos con elementos digitales***, prototipos de productos con elementos digitales o productos parcialmente completados con elementos digitales*** que no sean conformes ***con el***

	presente Reglamento, a condición de que el producto con elementos digitales en cuestión se utilice exclusivamente con fines de presentación en el curso del acto de que se trate, y de que una señal visible indique claramente su falta de conformidad con el presente Reglamento.

Enmienda 57

Propuesta de Reglamento
Artículo 4 – apartado 3

Texto de la Comisión	*Enmienda*
3. Los Estados miembros no impedirán la comercialización de ***programas informáticos*** inacabados que no sean conformes con el presente Reglamento, siempre que dichos programas solo se comercialicen ***durante un período de tiempo limitado, requerido*** a efectos de ensayo, y que se indique con claridad, mediante una señal visible, que no son conformes con el presente Reglamento y que no se comercializarán con fines distintos de su ensayo.	3. Los Estados miembros no impedirán la comercialización de ***productos con elementos digitales*** inacabados ***o de prototipos de productos con elementos digitales*** que no sean conformes con el presente Reglamento, siempre que dichos programas solo se comercialicen ***en una versión que no sea de producción*** a efectos de ensayo, y que se indique con claridad, mediante una señal visible, que no son conformes con el presente Reglamento y que no se comercializarán con fines distintos de su ensayo.

Enmienda 58

Propuesta de Reglamento
Artículo 4 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. El presente Reglamento no impedirá que los Estados miembros sometan a los productos con elementos digitales a otras medidas adicionales cuando los productos en cuestión se utilicen con fines militares, de defensa o de seguridad nacional, de conformidad con el Derecho nacional y de la Unión, y tales medidas sean necesarias y

	proporcionadas para la consecución de dichos fines.

Enmienda 59

Propuesta de Reglamento
Artículo 5 – párrafo 1 – punto 1

Texto de la Comisión	*Enmienda*
1) cumplen los requisitos esenciales establecidos en la sección 1 del anexo I, a condición de que hayan sido instalados de manera adecuada, mantenidos y utilizados para los fines previstos o en condiciones que se puedan prever razonablemente y, en su caso, ***actualizados***, y si	1) cumplen los requisitos esenciales establecidos en la sección 1 del anexo I, a condición de que hayan sido instalados de manera adecuada, mantenidos y utilizados para los fines previstos o en condiciones que se puedan prever razonablemente y, en su caso, ***reciban las actualizaciones de seguridad necesarias***, y si

Enmienda 60

Propuesta de Reglamento
Artículo 6 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los productos con elementos digitales que pertenezcan a una categoría mencionada en el anexo III se considerarán productos críticos con elementos digitales. Los productos que tengan una función principal de una categoría mencionada en el anexo III del presente Reglamento se considerarán incluidos en dicha categoría. Las categorías de productos críticos con elementos digitales se dividirán en las clases I y II, tal como se establece en el anexo III, para reflejar el nivel de riesgo de ciberseguridad asociado a dichos productos.	1. Los productos con elementos digitales que pertenezcan a una categoría mencionada en el anexo III se considerarán productos críticos con elementos digitales. ***Únicamente*** los productos que tengan una función principal de una categoría mencionada en el anexo III del presente Reglamento se considerarán incluidos en dicha categoría. Las categorías de productos críticos con elementos digitales se dividirán en las clases I y II, tal como se establece en el anexo III, para reflejar el nivel de riesgo de ciberseguridad asociado a dichos productos. ***La integración de un componente de una clase de criticidad superior en un producto de criticidad inferior no modifica necesariamente el nivel de criticidad del producto en el que se integre dicho componente.***

Enmienda 61

Propuesta de Reglamento
Artículo 6 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
b) el uso previsto en entornos sensibles***, en particular en entornos industriales*** o por parte de entidades esenciales contempladas en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)];	b) el uso previsto ***en aplicaciones críticas*** en entornos sensibles o por parte de entidades esenciales contempladas en el anexo [anexo I] de la Directiva [Directiva XXX/XXXX (SRI 2)];

Enmienda 62

Propuesta de Reglamento
Artículo 6 – apartado 2 – letra c

Texto de la Comisión	*Enmienda*
c) el uso ***previsto relativo*** a la realización de funciones críticas o sensibles, como el tratamiento de datos personales;	c) el uso ***y la escala previstos relativos*** a la realización de funciones críticas o sensibles, como el tratamiento de datos personales;

Enmienda 63

Propuesta de Reglamento
Artículo 6 – apartado 4

Texto de la Comisión	*Enmienda*
4. Los productos críticos con elementos digitales estarán sujetos a los procedimientos de evaluación de la conformidad especificados en el artículo 24, apartados 2 y 3.	4. Los productos críticos con elementos digitales estarán sujetos a los procedimientos de evaluación de la conformidad especificados en el artículo 24, apartados 2 y 3. ***Como excepción, las pequeñas empresas y las microempresas podrán utilizar el procedimiento a que se hace referencia en el artículo 24, apartado 2.***

Enmienda 64

Propuesta de Reglamento
Artículo 6 – apartado 5 – parte introductoria

Texto de la Comisión	*Enmienda*
5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 50 a fin de completar el presente Reglamento mediante el establecimiento de categorías de productos altamente críticos con elementos digitales, cuyos fabricantes ***deberán*** obtener un certificado europeo de ciberseguridad expedido en el marco de un esquema europeo de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 con el fin de demostrar la conformidad con los requisitos esenciales establecidos en el anexo I o parte de ellos. A la hora de determinar dichas categorías de productos altamente críticos con elementos digitales, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad asociado a la categoría de productos con elementos digitales, a la luz de uno o varios de los criterios enumerados en el apartado 2 y de la evaluación que determine si dicha categoría de productos:	5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 50 a fin de completar el presente Reglamento mediante el establecimiento de categorías de productos altamente críticos con elementos digitales, cuyos fabricantes ***podrán*** obtener un certificado europeo de ciberseguridad expedido en el marco de un esquema europeo de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881 con el fin de demostrar la conformidad con los requisitos esenciales establecidos en el anexo I o parte de ellos. A la hora de determinar dichas categorías de productos altamente críticos con elementos digitales, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad asociado a la categoría de productos con elementos digitales, a la luz de uno o varios de los criterios enumerados en el apartado 2 y de la evaluación que determine si dicha categoría de productos:

Enmienda 65

Propuesta de Reglamento
Artículo 8 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los productos con elementos digitales clasificados como sistemas de IA de alto riesgo de conformidad con el artículo [artículo 6] del Reglamento [Reglamento sobre IA] que entran en el ámbito de aplicación del presente Reglamento y cumplen los requisitos esenciales establecidos en la sección 1 del anexo I del presente Reglamento, siempre que los procesos establecidos por el fabricante cumplan los requisitos esenciales establecidos en la sección 2 del	1. Los productos con elementos digitales***, o los productos parcialmente completados con elementos digitales,*** clasificados como sistemas de IA de alto riesgo de conformidad con el artículo [artículo 6] del Reglamento [Reglamento sobre IA] que entran en el ámbito de aplicación del presente Reglamento y cumplen los requisitos esenciales establecidos en la sección 1 del anexo I del presente Reglamento, siempre que los procesos establecidos por el fabricante

anexo I, se considerarán conformes con los requisitos relativos a la ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA], sin perjuicio de los demás requisitos relativos a la precisión y la solidez incluidos en el citado artículo, en la medida en que la consecución del nivel de protección exigido por dichos requisitos se demuestre mediante la declaración UE de conformidad expedida en virtud del presente Reglamento.

cumplan los requisitos esenciales establecidos en la sección 2 del anexo I, se considerarán conformes con los requisitos relativos a la ciberseguridad establecidos en el artículo [artículo 15] del Reglamento [Reglamento sobre IA], sin perjuicio de los demás requisitos relativos a la precisión y la solidez incluidos en el citado artículo, en la medida en que la consecución del nivel de protección exigido por dichos requisitos se demuestre mediante la declaración UE de conformidad expedida en virtud del presente Reglamento.

Enmienda 66

Propuesta de Reglamento
Artículo 8 – apartado 2

Texto de la Comisión	*Enmienda*
2. Para los productos y los requisitos de ciberseguridad mencionados en el apartado 1, será aplicable el procedimiento de evaluación de la conformidad pertinente de conformidad con ***el artículo [artículo 43]*** del Reglamento [Reglamento sobre IA]. A efectos de dicha evaluación, los organismos notificados que dispongan de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA] también dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo incluidos en el ámbito de aplicación del presente Reglamento con los requisitos establecidos en su anexo I***, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos dispuestos en el artículo 29 del presente Reglamento en el contexto del procedimiento de notificación contemplado en el Reglamento [Reglamento sobre IA]***.	2. Para los productos y los requisitos de ciberseguridad mencionados en el apartado 1, será aplicable el procedimiento de evaluación de la conformidad pertinente de conformidad con ***las [disposiciones aplicables]*** del Reglamento [Reglamento sobre IA]. A efectos de dicha evaluación, los organismos notificados que dispongan de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo que entren en el ámbito de aplicación del Reglamento [Reglamento sobre IA] también dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo incluidos en el ámbito de aplicación del presente Reglamento con los requisitos establecidos en su anexo I.

Enmienda 67

Propuesta de Reglamento
Artículo 8 – apartado 3

Texto de la Comisión	*Enmienda*
3. No obstante lo dispuesto en el apartado 2, los productos críticos con elementos digitales enumerados en el anexo III del presente Reglamento que requieran la aplicación de los procedimientos de evaluación de la conformidad establecidos en el artículo 24, apartado 2, letras a) y b), y el artículo 24, apartado 3, letras a) y b), del presente Reglamento, que también estén clasificados como sistemas de IA de alto riesgo con arreglo al artículo [artículo 6] del Reglamento [Reglamento sobre IA] y a los que se aplique el procedimiento de evaluación de la conformidad basado en el control interno a que se refiere el anexo [anexo VI] del Reglamento [Reglamento sobre IA] estarán sujetos a los procedimientos de evaluación de la conformidad exigidos por el presente Reglamento en lo que respecta a los requisitos esenciales del presente Reglamento.	***suprimido***

Enmienda 68

Propuesta de Reglamento
Artículo 9 – párrafo 1

Texto de la Comisión	*Enmienda*
Las máquinas y sus partes y accesorios que entren en el ámbito de aplicación del Reglamento [propuesta de Reglamento sobre máquinas], que sean productos con elementos digitales en el sentido del presente Reglamento y para los que se haya expedido una declaración UE de conformidad sobre la base del presente Reglamento se presumirán conformes con los requisitos esenciales de salud y	Las máquinas y sus partes y accesorios que entren en el ámbito de aplicación del Reglamento [propuesta de Reglamento sobre máquinas], que sean productos con elementos digitales ***o productos parcialmente completados con elementos digitales*** en el sentido del presente Reglamento y para los que se haya expedido una declaración UE de conformidad sobre la base del presente

seguridad establecidos en el anexo [anexo III, secciones 1.1.9 y 1.2.1] del Reglamento [propuesta de Reglamento sobre máquinas], en lo que respecta a la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de mando, en la medida en que la declaración UE de conformidad emitida en virtud del presente Reglamento demuestre el cumplimiento del nivel de protección exigido por dichos requisitos.

Reglamento se presumirán conformes con los requisitos esenciales de salud y seguridad establecidos en el anexo [anexo III, secciones 1.1.9 y 1.2.1] del Reglamento [propuesta de Reglamento sobre máquinas], en lo que respecta a la protección contra la corrupción y la seguridad y fiabilidad de los sistemas de mando, en la medida en que la declaración UE de conformidad emitida en virtud del presente Reglamento demuestre el cumplimiento del nivel de protección exigido por dichos requisitos.

Enmienda 69

Propuesta de Reglamento
Artículo 10 – apartado –1 (nuevo)

Texto de la Comisión	*Enmienda*
	–1. Los fabricantes de programas informáticos que reúnan los requisitos para clasificarse como microempresas, según se definen en la Recomendación 2003/361/CE de la Comisión, harán cuando esté en su mano por cumplir los requisitos del presente Reglamento durante los seis meses posteriores a la comercialización de un programa informático. Esta disposición no se aplica a los productos altamente críticos con elementos digitales.

Enmienda 70

Propuesta de Reglamento
Artículo 10 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cuando se introduzca en el mercado un producto con elementos digitales, los fabricantes garantizarán que ha sido diseñado, desarrollado y ***producido*** de conformidad con los requisitos	1. Cuando se introduzca en el mercado un producto con elementos digitales, los fabricantes garantizarán que ha sido diseñado, desarrollado y ***fabricado*** de conformidad con los requisitos

esenciales establecidos en la sección 1 del anexo I.

esenciales establecidos en la sección 1 del anexo I.

Enmienda 71

Propuesta de Reglamento
Artículo 10 – apartado 4

Texto de la Comisión	*Enmienda*
4. A efectos del cumplimiento de la obligación establecida en el apartado 1, los fabricantes ejercerán la diligencia debida al integrar componentes procedentes de terceros en productos con elementos digitales. ***Velarán*** por que dichos componentes no comprometan la seguridad del producto con elementos digitales.	4. A efectos del cumplimiento de la obligación establecida en el apartado 1, los fabricantes ejercerán la diligencia debida al integrar componentes procedentes de terceros en productos con elementos digitales. ***Es responsabilidad del fabricante velar*** por que dichos componentes no comprometan la seguridad del producto con elementos digitales.

Enmienda 72

Propuesta de Reglamento
Artículo 10 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. Los fabricantes de los componentes facilitarán la información y la documentación necesarias para cumplir los requisitos del presente Reglamento cuando suministren dichos componentes al fabricante de los productos finales. Dicha información se ofrecerá de manera gratuita.

Enmienda 73

Propuesta de Reglamento
Artículo 10 – apartado 6 – párrafo 1

Texto de la Comisión	*Enmienda*
Desde la introducción de un producto con elementos digitales en el mercado y	Desde la introducción de un producto con elementos digitales en el mercado y

durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto en el mercado, si este período fuese más ***breve***, los fabricantes velarán por que las vulnerabilidades de dicho producto se gestionen de manera eficaz y de conformidad con los requisitos esenciales establecidos en la sección 2 del anexo I.	durante la vida útil prevista del producto ***en la fecha de su comercialización*** o durante cinco años a partir de la introducción del producto en el mercado, si este período fuese más ***prolongado***, los fabricantes velarán por que las vulnerabilidades de dicho producto se gestionen de manera eficaz y de conformidad con los requisitos esenciales establecidos en la sección 2 del anexo I***, siempre que esté bajo el control de los fabricantes***.

Enmienda 74

Propuesta de Reglamento
Artículo 10 – apartado 7 – párrafo 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Cuando se ejecuten actualizaciones de programas informáticos, el fabricante no estará obligado a efectuar otra evaluación de conformidad del producto con elementos digitales, salvo que la actualización de que se trate dé lugar a una modificación sustancial de dicho producto en el sentido de lo dispuesto en el artículo 3, punto 31, del presente Reglamento.

Enmienda 75

Propuesta de Reglamento
Artículo 10 – apartado 9

Texto de la Comisión	*Enmienda*
9. Los fabricantes se asegurarán de que existan procedimientos para que los productos con elementos digitales que formen parte de una producción en serie mantengan su conformidad. El fabricante tomará debidamente en consideración los cambios en el proceso de desarrollo y producción o en el diseño o las características del producto con elementos	9. Los fabricantes se asegurarán de que existan procedimientos para que los productos con elementos digitales que formen parte de una producción en serie mantengan su conformidad. El fabricante tomará debidamente en consideración los cambios en el proceso de desarrollo y producción o en el diseño o las características del producto con elementos

digitales, así como los cambios en las normas armonizadas, en los esquemas europeos de certificación de la ciberseguridad o en las especificaciones técnicas a que se hace referencia en el artículo 19 en virtud de las cuales se declara o por aplicación de las cuales se verifica la conformidad del producto.	digitales, así como los cambios en las normas armonizadas, en los esquemas europeos de certificación de la ciberseguridad o en las especificaciones técnicas a que se hace referencia en el artículo 19 en virtud de las cuales se declara o por aplicación de las cuales se verifica la conformidad del producto. ***Cuando estén disponibles nuevos conocimientos, técnicas o normas que no lo estaban en el momento del diseño de un producto en serie, el fabricante podrá considerar la implantación de tales mejoras periódicamente respecto a futuras generaciones de productos.***

Enmienda 76

Propuesta de Reglamento
Artículo 10 – apartado 9 bis (nuevo)

Texto de la Comisión	*Enmienda*
	9 bis. Los fabricantes comunicarán públicamente la vida útil prevista de sus productos de un modo claro y comprensible.

Enmienda 77

Propuesta de Reglamento
Artículo 10 – apartado 12

Texto de la Comisión	*Enmienda*
12. Desde la introducción en el mercado de un producto con elementos digitales y durante la vida útil prevista del producto o durante cinco años a partir de la introducción en el mercado del producto, si este período fuese más ***breve***, los fabricantes que sepan o tengan motivos para creer que el producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales establecidos en el	12. Desde la introducción en el mercado de un producto con elementos digitales y durante la vida útil prevista del producto o durante cinco años a partir de la introducción en el mercado del producto, si este período fuese más ***prolongado***, los fabricantes que sepan o tengan motivos para creer que el producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales establecidos en el

anexo I adoptarán inmediatamente las medidas correctoras necesarias para que el producto con elementos digitales o los procesos del fabricante sean conformes, para retirarlo del mercado o para recuperarlo, según proceda.

anexo I adoptarán inmediatamente las medidas correctoras necesarias para que el producto con elementos digitales o los procesos del fabricante sean conformes, para retirarlo del mercado o para recuperarlo, según proceda.

Enmienda 78

Propuesta de Reglamento
Artículo 11 – apartado 1

Texto de la Comisión	*Enmienda*
1. El fabricante notificará a la ENISA, sin demora indebida, y en cualquier caso en un plazo de ***veinticuatro*** horas a partir del momento en que tenga conocimiento de ello, cualquier vulnerabilidad aprovechada activamente presente en el producto con elementos digitales. ***La notificación incluirá información detallada sobre dicha vulnerabilidad y, en su caso, sobre las medidas correctoras o paliativas adoptadas. La ENISA transmitirá la notificación tras su recepción, sin demora indebida salvo por motivos justificados en relación con los riesgos de ciberseguridad, al CSIRT designado a efectos de la divulgación coordinada de vulnerabilidades con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará a la autoridad de vigilancia del mercado sobre la vulnerabilidad notificada.***	1. El fabricante notificará a la ENISA, sin demora indebida, y en cualquier caso en un plazo de ***cuarenta y ocho*** horas a partir del momento en que tenga conocimiento de ello, ***mediante una alerta temprana,*** cualquier vulnerabilidad aprovechada activamente presente en el producto con elementos digitales.

Enmienda 79

Propuesta de Reglamento
Artículo 11 – apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. El fabricante proporcionará a la ENISA, sin demora indebida a partir del

momento en que tenga conocimiento de una vulnerabilidad aprovechada que afecte de manera significativa a la seguridad del producto con elementos digitales, información pormenorizada adicional sobre la vulnerabilidad de que se trate.

Enmienda 80

Propuesta de Reglamento
Artículo 11 – apartado 1 ter (nuevo)

Texto de la Comisión	*Enmienda*
	1 ter. Todas las demás vulnerabilidades que no afecten de manera significativa a la seguridad del producto con elementos digitales se notificarán a la ENISA una vez que se haya abordado la vulnerabilidad.

Enmienda 81

Propuesta de Reglamento
Artículo 11 – apartado 1 quater (nuevo)

Texto de la Comisión	*Enmienda*
	1 quater. La notificación incluirá información detallada sobre dicha vulnerabilidad y, en su caso, sobre las medidas correctoras o paliativas adoptadas y las medidas de mitigación del riesgo recomendadas. La ENISA transmitirá la notificación tras su recepción, sin demora indebida salvo por motivos justificados en relación con los riesgos de ciberseguridad, al CSIRT designado a efectos de la divulgación coordinada de vulnerabilidades con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará inmediatamente a la autoridad de vigilancia del mercado sobre la

existencia de una vulnerabilidad y, cuando proceda, de las posibles medidas de mitigación del riesgo. Si para una vulnerabilidad notificada no hay disponibles medidas correctoras o de mitigación, la ENISA velará por que la información sobre la vulnerabilidad notificada se comunique en línea con unos estrictos protocolos de seguridad y según la necesidad de conocerla.

Enmienda 82

Propuesta de Reglamento
Artículo 11 – apartado 2

Texto de la Comisión	*Enmienda*
2. El fabricante notificará a la ENISA**,** sin demora indebida, y en cualquier caso en un plazo de veinticuatro horas a partir del momento en que tenga conocimiento de ello, cualquier incidente que afecte al producto con elementos digitales. La ENISA transmitirá la notificación, sin demora indebida, salvo por motivos justificados en relación con los riesgos de ciberseguridad, al punto único de contacto designado con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará a la autoridad de vigilancia del mercado sobre los incidentes notificados. La notificación del incidente incluirá información sobre la gravedad y las repercusiones del incidente y, en su caso, indicará si el fabricante sospecha que el incidente ha sido causado por actos ilícitos o malintencionados o si considera que tiene repercusiones transfronterizas.	2. El fabricante notificará a la ENISA sin demora indebida, y en cualquier caso en un plazo de veinticuatro horas a partir del momento en que tenga conocimiento de ello, ***mediante una alerta temprana,*** cualquier incidente que afecte ***de manera significativa*** al producto con elementos digitales. ***El fabricante proporcionará a la ENISA, sin demora indebida, y en cualquier caso en un plazo de setenta y dos horas a partir del momento en que tenga conocimiento del incidente significativo relacionado con el producto con elementos digitales, información pormenorizada adicional sobre el incidente significativo de que se trate.*** La ENISA transmitirá la notificación, sin demora indebida, salvo por motivos justificados en relación con los riesgos de ciberseguridad, al punto único de contacto designado con arreglo al artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] de los Estados miembros afectados e informará ***de inmediato*** a la autoridad de vigilancia del mercado sobre los incidentes ***significativos*** notificados. La notificación del incidente incluirá ***la*** información ***que resulte estrictamente necesaria para que la autoridad competente adquiera***

	conocimiento del incidente, y cuando proceda y sea proporcional al riesgo, sobre la gravedad y las repercusiones del incidente y, en su caso, indicará si el fabricante sospecha que el incidente ha sido causado por actos ilícitos o malintencionados o si considera que tiene repercusiones transfronterizas. ***El mero acto de notificar no elevará la responsabilidad de la entidad notificante.***

Enmienda 83

Propuesta de Reglamento
Artículo 11 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. Deberá considerarse que los operadores económicos a los que se identifique además como entidades esenciales o importantes en la Directiva SRI 2 y que presenten sus notificaciones de incidentes con arreglo a dicha Directiva, cumplen los requisitos formulados en el apartado 2 del presente artículo.

Enmienda 84

Propuesta de Reglamento
Artículo 11 – apartado 3

Texto de la Comisión	*Enmienda*
3. La ENISA presentará a la red de organizaciones de enlace para la gestión de cibercrisis de la UE (CyCLONe) creada por el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] la información notificada con arreglo a los apartados 1 y 2 si dicha información es pertinente para la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo.	3. La ENISA presentará a la red de organizaciones de enlace para la gestión de cibercrisis de la UE (CyCLONe) creada por el artículo [artículo X] de la Directiva [Directiva XXX/XXXX (SRI 2)] la información notificada con arreglo a los apartados 1 y 2 si dicha información es pertinente para la gestión coordinada de incidentes ***significativos*** y crisis de ciberseguridad a gran escala a nivel operativo.

Enmienda 85

Propuesta de Reglamento
Artículo 11 – apartado 4

Texto de la Comisión	*Enmienda*
4. El fabricante informará, sin demora indebida y una vez tenga conocimiento de ello, a los usuarios del producto con elementos digitales sobre el incidente y, cuando así se requiera, sobre las medidas correctoras que el usuario pueda adoptar para mitigar las repercusiones del incidente.	4. El fabricante informará, sin demora indebida y una vez tenga conocimiento de ello, a los usuarios del producto con elementos digitales sobre el incidente ***significativo, cuando proceda y sea probable que les afecte negativamente,*** y, cuando así se requiera, sobre las medidas ***de mitigación del riesgo y medidas*** correctoras que el usuario pueda adoptar para mitigar las repercusiones del incidente ***significativo en relación con los posibles datos afectados y los daños potenciales***.

Enmienda 86

Propuesta de Reglamento
Artículo 11 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. Las obligaciones previstas en los apartados 1, 2 y 4 se aplicarán a lo largo de la vida útil del producto. Durante el período previsto de vida útil del producto, el fabricante ofrecerá actualizaciones de seguridad de manera gratuita, que se aplicarán únicamente a los productos con elementos digitales respecto a los que el fabricante haya elaborado una declaración UE de conformidad, con arreglo al artículo 20 del presente Reglamento.

Enmienda 87

Propuesta de Reglamento
Artículo 11 – apartado 5

Texto de la Comisión	*Enmienda*
5. La Comisión podrá, mediante actos de ejecución, especificar el tipo de información, el formato y el procedimiento de las notificaciones presentadas con arreglo a los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.	5. La Comisión***, tras consultar a las partes interesadas y los CSIRT,*** podrá, mediante actos de ejecución, especificar el tipo de información, el formato y el procedimiento de las notificaciones presentadas con arreglo a los apartados 1 y 2. Dichos actos de ejecución ***se basarán en las normas europeas e internacionales y*** se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 51, apartado 2.

Enmienda 88

Propuesta de Reglamento
Artículo 11 – apartado 6

Texto de la Comisión	*Enmienda*
6. Sobre la base de las notificaciones recibidas con arreglo a los apartados 1 y 2, la ENISA elaborará un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en los productos con elementos digitales y lo presentará al Grupo de Cooperación especificado en el artículo ***[artículo X]*** de la Directiva ***[Directiva XXX/XXXX (SRI 2)]***. El primero de estos informes se presentará en un plazo de veinticuatro meses a partir de la fecha en que empiecen a ser aplicables las obligaciones establecidas en los apartados 1 y 2.	6. Sobre la base de las notificaciones recibidas con arreglo a los apartados 1 y 2, la ENISA elaborará un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en los productos con elementos digitales y lo presentará al Grupo de Cooperación especificado en el artículo ***14*** de la Directiva ***(UE) 2022/2555***. El primero de estos informes se presentará en un plazo de veinticuatro meses a partir de la fecha en que empiecen a ser aplicables las obligaciones establecidas en los apartados 1 y 2.

Enmienda 89

Propuesta de Reglamento
Artículo 11 – apartado 7

Texto de la Comisión	*Enmienda*
7. Al detectar una vulnerabilidad en un componente, incluso si este es de	7. Al detectar una vulnerabilidad en un componente, incluso si este es de

código abierto, integrado en el producto con elementos digitales, los fabricantes notificarán la vulnerabilidad a la persona o entidad a cargo del mantenimiento del componente.	código abierto, integrado en el producto con elementos digitales, los fabricantes notificarán la vulnerabilidad ***y la medida correctiva o de mitigación adoptada*** a la persona o entidad a cargo del mantenimiento del componente. ***Ello no exime al fabricante de la obligación de mantener la conformidad del producto con los requisitos del presente Reglamento, ni crea obligaciones a los desarrolladores de componentes libres y de código abierto que carezcan de una relación contractual con el fabricante en cuestión.***

Enmienda 90

Propuesta de Reglamento
Artículo 12 – apartado 3 – parte introductoria

Texto de la Comisión	*Enmienda*
3. El representante autorizado efectuará las tareas especificadas en el mandato recibido del fabricante. El mandato permitirá al representante autorizado realizar como mínimo las tareas siguientes:	3. El representante autorizado efectuará las tareas especificadas en el mandato recibido del fabricante. ***Facilitará a las autoridades de vigilancia del mercado, siempre que estas lo soliciten, una copia del mandato.*** El mandato permitirá al representante autorizado realizar como mínimo las tareas siguientes:

Enmienda 91

Propuesta de Reglamento
Artículo 12 – apartado 3 – letra a bis (nueva)

Texto de la Comisión	*Enmienda*
	a bis) cuando el representante autorizado tenga motivos para creer que el producto con elementos digitales en cuestión presenta un riesgo de ciberseguridad, informar de ello al fabricante;

Enmienda 92

Propuesta de Reglamento
Artículo 12 – apartado 3 – letra b

Texto de la Comisión	*Enmienda*
b) en respuesta a una solicitud motivada de una autoridad de vigilancia del mercado, facilitar a dicha autoridad toda la información y documentación necesarias para demostrar la conformidad del producto con elementos digitales;	b) en respuesta a una solicitud motivada de una autoridad de vigilancia del mercado, facilitar a dicha autoridad toda la información y documentación necesarias para demostrar ***la seguridad y*** la conformidad del producto con elementos digitales ***en una lengua que pueda entender fácilmente dicha autoridad***;

Enmienda 93

Propuesta de Reglamento
Artículo 12 – apartado 3 – letra c

Texto de la Comisión	*Enmienda*
c) cooperar con las autoridades de vigilancia del mercado, a petición de estas, en cualquier acción destinada a eliminar los riesgos que presente un producto con elementos digitales objeto del mandato del representante autorizado**.**	c) cooperar con las autoridades de vigilancia del mercado, a petición de estas, en cualquier acción destinada a eliminar ***de manera efectiva*** los riesgos que presente un producto con elementos digitales objeto del mandato del representante autorizado***;***

Enmienda 94

Propuesta de Reglamento
Artículo 13 – apartado 2 – letra c bis (nueva)

Texto de la Comisión	*Enmienda*
	c bis) todos los documentos que acrediten el cumplimiento de los requisitos establecidos en el presente artículo se han recibido del fabricante y se encuentran disponibles para su inspección por un período de diez años.

Enmienda 95

Propuesta de Reglamento
Artículo 13 – apartado 3

Texto de la Comisión	*Enmienda*
3. Si un importador considera o tiene motivos para creer que un producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales establecidos en el anexo I, no lo introducirá en el mercado hasta que el producto o los procesos establecidos por el fabricante no se hayan llevado a la conformidad con los requisitos esenciales establecidos en el anexo I. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, el importador informará de ello al fabricante y a las autoridades de vigilancia del mercado.	3. Si un importador considera o tiene motivos para creer***, con arreglo a la información de la que dispone,*** que un producto con elementos digitales o los procesos establecidos por el fabricante no son conformes con los requisitos esenciales establecidos en el anexo I, no lo introducirá en el mercado hasta que el producto o los procesos establecidos por el fabricante no se hayan llevado a la conformidad con los requisitos esenciales establecidos en el anexo I. Además, cuando el producto con elementos digitales presente un riesgo de ciberseguridad significativo, el importador informará de ello al fabricante y a las autoridades de vigilancia del mercado.

Enmienda 96

Propuesta de Reglamento
Artículo 13 – apartado 4

Texto de la Comisión	*Enmienda*
4. Los importadores indicarán su nombre, nombre comercial registrado o marca registrada, su dirección postal y su dirección de correo electrónico de contacto en el producto con elementos digitales o, cuando no sea posible, en su embalaje o en un documento que acompañe al producto con elementos digitales. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios finales y las autoridades de vigilancia del mercado.	4. Los importadores indicarán su nombre, ***su*** nombre comercial registrado o marca registrada, su dirección postal y su dirección de correo electrónico de contacto en el producto con elementos digitales o, cuando no sea posible, en su embalaje o en un documento que acompañe al producto con elementos digitales. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios finales y las autoridades de vigilancia del mercado.

Enmienda 97

Propuesta de Reglamento
Artículo 13 – apartado 6 – párrafo 1

Texto de la Comisión	*Enmienda*
Los importadores que sepan o tengan motivos para creer que un producto con elementos digitales que han introducido en el mercado o los procesos establecidos por su fabricante no son conformes con los requisitos esenciales establecidos en el anexo I adoptarán inmediatamente las medidas correctoras necesarias para que dicho producto con elementos digitales o los procesos establecidos por su fabricante sean conformes con los requisitos esenciales establecidos en el anexo I, o bien para retirarlo del mercado o recuperarlo, cuando proceda.	Los importadores que sepan o tengan motivos para creer que un producto con elementos digitales que han introducido en el mercado o los procesos establecidos por su fabricante no son conformes con los requisitos esenciales establecidos en el anexo I adoptarán inmediatamente las medidas correctoras necesarias para que dicho producto con elementos digitales o los procesos establecidos por su fabricante sean conformes con los requisitos esenciales establecidos en el anexo I, o bien para retirarlo del mercado o recuperarlo, cuando proceda. ***Sobre la base de una evaluación de riesgos, a los distribuidores y a los usuarios finales se les informará puntualmente de la falta de conformidad y de las medidas de mitigación de riesgos que pueden adoptar.***

Enmienda 98

Propuesta de Reglamento
Artículo 14 – apartado 2 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) han recibido del fabricante o del importador toda la información y la documentación requeridas con arreglo al presente Reglamento.

Enmienda 99

Propuesta de Reglamento
Artículo 16 – párrafo 1

Texto de la Comisión	*Enmienda*
A los efectos del presente Reglamento, se considerará fabricante a una persona física	A los efectos del presente Reglamento, se considerará fabricante a una persona física

o jurídica, distinta del fabricante, el importador o el distribuidor, que lleve a cabo una modificación sustancial del producto con elementos digitales.	o jurídica, distinta del fabricante, el importador o el distribuidor, que***, en el desempeño de una actividad profesional,*** lleve a cabo una modificación sustancial del producto con elementos digitales ***y lo comercialice***.

Enmienda 100

Propuesta de Reglamento
Artículo 18 – apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. En virtud de lo dispuesto en el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, la Comisión solicitará que una o varias organizaciones europeas de normalización elaboren normas armonizadas relativas a los requisitos establecidos en el anexo I.

Enmienda 101

Propuesta de Reglamento
Artículo 18 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. De conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, al preparar la petición de normalización para los productos en el ámbito de aplicación del presente Reglamento, la Comisión aspirará a la máxima armonización con las normas internacionales vigentes o inminentes en materia de ciberseguridad. En los tres primeros años posteriores a la fecha de aplicación del presente Reglamento, la Comisión estará facultada para declarar una norma internacional existente como conforme con los requisitos del presente Reglamento, sin modificaciones europeas, a condición de que la observancia de tales normas refuerce suficientemente la

seguridad de los productos con elementos digitales, y de que la norma se publique como una versión separada por uno de los organismos europeos de normalización.

Enmienda 102

Propuesta de Reglamento
Artículo 19 – párrafo 1

Texto de la Comisión	*Enmienda*
Cuando no existan las normas armonizadas mencionadas en el artículo 18, cuando la Comisión considere que las normas armonizadas pertinentes son insuficientes para cumplir los requisitos del presente Reglamento o ajustarse a la petición de normalización de la Comisión, cuando se produzcan demoras indebidas en el procedimiento de normalización o cuando la solicitud de normas armonizadas por parte de la Comisión no haya sido aceptada por las organizaciones europeas de normalización, la Comisión estará facultada para adoptar***, mediante*** actos de ejecución***,*** especificaciones comunes con respecto a los requisitos ***esenciales*** establecidos en el anexo I. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo ***51***, apartado ***2***.	***1.*** La Comisión estará facultada para adoptar actos de ejecución ***por los que se establezcan*** especificaciones comunes relativas a los requisitos ***técnicos que proporcionen un medio para cumplir los requisitos esenciales de salud y seguridad*** establecidos en el anexo I ***para los productos incluidos en el ámbito de aplicación del presente Reglamento. Dichos actos de ejecución solo se adoptarán cuando se cumplan las condiciones siguientes:***
	a) la Comisión, en virtud de lo dispuesto en el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, ha solicitado que una o varias organizaciones europeas de normalización elaboren una norma armonizada relativa a los requisitos esenciales establecidos en el anexo I y:
	i) la solicitud no se haya aceptado; o
	ii) las normas armonizadas que respondan a esa solicitud no se hayan entregado en el plazo establecido de conformidad con el artículo 10,

apartado 1, del Reglamento (UE) n.º 1025/2012; o

iii) las normas armonizadas incumplan la solicitud; y

b) no se haya publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que regulen los requisitos establecidos en el anexo I de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevea la publicación de ninguna referencia en un plazo razonable.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo ***48***, apartado ***3***.

Enmienda 103

Propuesta de Reglamento
Artículo 19 – párrafo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. Antes de preparar el proyecto de acto delegado a que se refiere el apartado 3, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 3.

Enmienda 104

Propuesta de Reglamento
Artículo 19 – párrafo 1 ter (nuevo)

Texto de la Comisión	*Enmienda*
	1 ter. Al preparar el proyecto de acto de ejecución a que se refiere el apartado 1, la Comisión tendrá en cuenta los puntos de vista de los organismos pertinentes o del grupo de expertos y consultará debidamente a todas las partes interesadas

pertinentes.

Enmienda 105

Propuesta de Reglamento
Artículo 19 – párrafo 1 quater (nuevo)

Texto de la Comisión	*Enmienda*
	1 quater. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el Diario Oficial de la Unión Europea, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando se publique la referencia de una norma armonizada en el Diario Oficial de la Unión Europea, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o las partes de estos que prevean los mismos requisitos que prevé dicha norma armonizada.

Enmienda 106

Propuesta de Reglamento
Artículo 19 – párrafo 1 quinquies (nuevo)

Texto de la Comisión	*Enmienda*
	1 quinquies. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en el anexo I, informará de ello a la Comisión presentando una explicación detallada. La Comisión evaluará dicha explicación detallada y, si procede, podrá modificar el acto de ejecución por el que se establezca la especificación común en cuestión.

Enmienda 107

Propuesta de Reglamento
Artículo 20 – apartado 2

Texto de la Comisión	*Enmienda*
2. La declaración UE de conformidad tendrá la estructura tipo establecida en el anexo IV y contendrá los elementos especificados en los procedimientos de evaluación de la conformidad correspondientes establecidos en el anexo VI. La declaración se mantendrá ***permanentemente*** actualizada. Estará disponible en ***la*** lengua ***o las lenguas requeridas por el*** Estado miembro en cuyo mercado se introduzca o se comercialice el producto con elementos digitales.	2. La declaración UE de conformidad tendrá la estructura tipo establecida en el anexo IV y contendrá los elementos especificados en los procedimientos de evaluación de la conformidad correspondientes establecidos en el anexo VI. La declaración se mantendrá actualizada ***como corresponda***. Estará disponible en ***una*** lengua ***que puedan comprender fácilmente las autoridades del*** Estado miembro en cuyo mercado se introduzca o se comercialice el producto con elementos digitales.

Enmienda 108

Propuesta de Reglamento
Artículo 20 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 20 bis
	Declaración UE de incorporación para productos parcialmente completados con elementos digitales
	1. Los fabricantes elaborarán la declaración UE de incorporación con arreglo a lo dispuesto en el artículo 10, apartado 7, y harán constar que se ha demostrado el cumplimiento de los requisitos esenciales aplicables establecidos en el anexo I.
	2. La declaración UE de incorporación tendrá la estructura tipo que se establece en el anexo IV bis (nuevo). La declaración se mantendrá actualizada como corresponda. Estará disponible en la lengua o las lenguas requeridas por el Estado miembro en cuyo

mercado se introduzca o se comercialice el producto parcialmente completado con elementos digitales.

3. Cuando un producto parcialmente completado con elementos digitales esté sujeto a más de un acto de la Unión que exija una declaración UE de incorporación, se elaborará una única declaración UE de incorporación con respecto a todos esos actos de la Unión. Dicha declaración contendrá la identificación de los actos de la Unión correspondientes y sus referencias de publicación.

4. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de completar el presente Reglamento mediante la inclusión de elementos al contenido mínimo de la declaración UE de incorporación establecido en el anexo IV bis (nuevo) a fin de tener en cuenta los avances tecnológicos.

Enmienda 109

Propuesta de Reglamento
Artículo 22 – apartado 1

Texto de la Comisión	*Enmienda*
1. El marcado CE se colocará en el producto con elementos digitales de manera visible, legible e indeleble. Cuando ello no sea posible o no se justifique dada la naturaleza del producto con elementos digitales, se colocará en el embalaje y en la declaración UE de conformidad mencionada en el artículo 20 que acompañen al producto con elementos digitales. En el caso de los productos con elementos digitales en forma de programas informáticos, el marcado CE se colocará en la declaración UE de conformidad mencionada en el artículo 20 o el sitio web que acompañen al producto.	1. El marcado CE se colocará en el producto con elementos digitales de manera visible, legible e indeleble. Cuando ello no sea posible o no se justifique dada la naturaleza del producto con elementos digitales, se colocará en el embalaje y en la declaración UE de conformidad mencionada en el artículo 20 que acompañen al producto con elementos digitales. En el caso de los productos con elementos digitales en forma de programas informáticos, el marcado CE se colocará en la declaración UE de conformidad mencionada en el artículo 20 o el sitio web que acompañen al producto. ***En este último caso, los consumidores podrán acceder de***

	manera sencilla y directa al apartado pertinente del sitio web.

Enmienda 110

Propuesta de Reglamento
Artículo 22 – apartado 3

Texto de la Comisión	*Enmienda*
3. El marcado CE se colocará antes de que el producto con elementos digitales se introduzca en el mercado. Podrá ir seguido de un pictograma o cualquier otra marca que indique un riesgo o uso especial establecido en los actos de ejecución a que se refiere el apartado 6.	3. El marcado CE se colocará antes de que el producto con elementos digitales se introduzca en el mercado. Podrá ir seguido de un pictograma o cualquier otra marca que indique ***a los consumidores*** un riesgo o uso especial establecido en los actos de ejecución a que se refiere el apartado 6.

Enmienda 111

Propuesta de Reglamento
Artículo 22 – apartado 5

Texto de la Comisión	*Enmienda*
5. Los Estados miembros se basarán en los mecanismos existentes para garantizar la correcta ***aplicación*** del régimen que regula el marcado CE y adoptarán las medidas adecuadas en caso de uso indebido de dicho marcado. Cuando el producto con elementos digitales esté sujeto a otras disposiciones legislativas de la Unión que también requieran la colocación del marcado CE, este indicará que el producto también cumple los requisitos de esas otras disposiciones legislativas.	5. Los Estados miembros se basarán en los mecanismos existentes para garantizar la ***aplicación*** correcta ***y armonizada*** del régimen que regula el marcado CE y adoptarán las medidas adecuadas ***y coordinadas*** en caso de uso indebido de dicho marcado. Cuando el producto con elementos digitales esté sujeto a otras disposiciones legislativas de la Unión que también requieran la colocación del marcado CE, este indicará que el producto también cumple los requisitos de esas otras disposiciones legislativas.

Enmienda 112

Propuesta de Reglamento
Artículo 22 – apartado 6

Texto de la Comisión	*Enmienda*
6. La Comisión podrá, mediante actos ***de ejecución***, establecer especificaciones técnicas para pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales, así como mecanismos para promover su uso. Dichos actos ***de ejecución*** se adoptarán de conformidad con el procedimiento ***de examen*** a que se refiere el artículo ***51, apartado 2***.	6. La Comisión podrá, mediante actos ***delegados***, establecer especificaciones técnicas para ***sistemas de etiquetado, incluidas las etiquetas armonizadas,*** pictogramas o cualquier otro marcado relativo a la seguridad de los productos con elementos digitales, así como mecanismos para promover su uso ***entre las empresas y los consumidores y fomentar la sensibilización pública respecto a la seguridad de los productos con elementos digitales***. Dichos actos ***delegados*** se adoptarán de conformidad con el procedimiento a que se refiere el artículo ***50***.

Enmienda 113

Propuesta de Reglamento
Artículo 22 – apartado 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	6 bis. Un producto parcialmente completado con elementos digitales no se marcará con el marcado CE conforme al presente Reglamento, sin perjuicio de las disposiciones sobre marcado que se deriven de otra legislación aplicable de la Unión.

Enmienda 114

Propuesta de Reglamento
Artículo 22 – apartado 6 ter (nuevo)

Texto de la Comisión	*Enmienda*
	6 ter. La Comisión adoptará directrices y proporcionará asesoramiento a los operadores económicos, en particular a los que cumplan los requisitos para ser considerados pymes, incluidas las

	microempresas, sobre la aplicación del presente Reglamento. En particular, las directrices y el asesoramiento tendrán por objeto simplificar y limitar las cargas administrativas y financieras, asegurando al mismo tiempo una aplicación eficaz y coherente del presente Reglamento de conformidad con el objetivo general de garantizar la seguridad de los productos y la protección de los consumidores. La Comisión debe consultar a las partes interesadas pertinentes con conocimientos técnicos en el ámbito de la ciberseguridad.

Enmienda 115

Propuesta de Reglamento
Artículo 23 – apartado 2

Texto de la Comisión	*Enmienda*
2. La documentación técnica se elaborará antes de que el producto con elementos digitales se introduzca en el mercado y, en su caso, se mantendrá permanentemente actualizada durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto con elementos digitales en el mercado, si este período fuese más ***breve***.	2. La documentación técnica se elaborará antes de que el producto con elementos digitales se introduzca en el mercado y, en su caso, se mantendrá permanentemente actualizada durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto con elementos digitales en el mercado, si este período fuese más ***prolongado***.

Enmienda 116

Propuesta de Reglamento
Artículo 23 – apartado 3

Texto de la Comisión	*Enmienda*
3. En el caso de los productos con elementos digitales ***a que se refieren el artículo 8 y el artículo 24, apartado 4,*** que también estén sujetos a otros actos de la Unión, se elaborará una única documentación técnica que contenga la información a que hace referencia el	3. En el caso de los productos con elementos digitales que también estén sujetos a otros actos de la Unión, se elaborará una única documentación técnica que contenga la información a que hace referencia el anexo V del presente Reglamento y la información requerida por

anexo V del presente Reglamento y la información requerida por esos actos de la Unión respectivos.

esos actos de la Unión respectivos.

Enmienda 117

Propuesta de Reglamento
Artículo 23 – apartado 5

Texto de la Comisión	*Enmienda*
5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de completar el presente Reglamento mediante la inclusión de elementos en la documentación técnica establecida en el anexo V a fin de tener en cuenta los avances tecnológicos, así como los imprevistos que surjan durante el proceso de ejecución del presente Reglamento.	5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 50 a fin de completar el presente Reglamento mediante la inclusión de elementos en la documentación técnica establecida en el anexo V a fin de tener en cuenta los avances tecnológicos, así como los imprevistos que surjan durante el proceso de ejecución del presente Reglamento. ***La Comisión procurará reducir al mínimo la carga administrativa, en especial para las microempresas y las pequeñas y medianas empresas.***

Enmienda 118

Propuesta de Reglamento
Artículo 24 – apartado 1 – letra c bis (nueva)

Texto de la Comisión	*Enmienda*
	c bis) un esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 18, apartado 4, del Reglamento (UE) 2019/881.

Enmienda 119

Propuesta de Reglamento
Artículo 24 – apartado 3 – letra b

Texto de la Comisión	*Enmienda*
b) evaluación de la conformidad basada en el aseguramiento de calidad total (basada en el módulo H) que se establece en el anexo VI**.**	b) evaluación de la conformidad basada en el aseguramiento de calidad total (basada en el módulo H) que se establece en el anexo VI***; o***

Enmienda 120

Propuesta de Reglamento
Artículo 24 – apartado 3 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) en su caso, un esquema europeo de certificación de la ciberseguridad a un nivel de garantía «sustancial» o «elevada» con arreglo al Reglamento (UE) 2019/881.

Enmienda 121

Propuesta de Reglamento
Artículo 24 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. En el caso de los productos a los que se aplique la legislación de armonización de la Unión basada en el nuevo marco legislativo, el fabricante se atendrá a la evaluación de conformidad pertinente que se exija en tales actos legislativos. Los requisitos formulados en el capítulo III se aplicarán a tales productos.

Enmienda 122

Propuesta de Reglamento
Artículo 24 – apartado 5

Texto de la Comisión	*Enmienda*
5. Los organismos notificados tendrán en cuenta los intereses y las necesidades específicos de las pequeñas y medianas empresas ***(pymes)*** a la hora de fijar las tasas que aplican a los procedimientos de evaluación de la conformidad y reducirán dichas tasas de forma proporcionada a dichos intereses y necesidades específicos.	5. Los organismos notificados tendrán en cuenta los intereses y las necesidades específicos de las ***microempresas y de las*** pequeñas y medianas empresas a la hora de fijar las tasas que aplican a los procedimientos de evaluación de la conformidad y reducirán dichas tasas de forma proporcionada a dichos intereses y necesidades específicos. ***La Comisión emprenderá acciones encaminadas a garantizar procedimientos más accesibles y asequibles, así como el apoyo financiero adecuado en el marco de los programas vigentes de la Unión, en particular con el fin de aliviar la carga que soportan las microempresas y las pequeñas y medianas empresas.***

Enmienda 123

Propuesta de Reglamento
Artículo 24 – apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. En el caso de los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento y que se introduzcan en el mercado o se pongan en servicio por entidades de crédito reguladas por la Directiva 2013/36/UE, la evaluación de la conformidad se llevará a cabo como parte del procedimiento a que se refieren los artículos 97 a 101 de dicha Directiva.

Enmienda 124

Propuesta de Reglamento
Artículo 24 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 24 bis
	Cuando los productos con elementos digitales posean equipos o programas informáticos equivalentes, un modelo de producto podrá ser representativo de una familia de productos a efectos de los siguientes procedimientos de evaluación de la conformidad:
	a) procedimiento de control interno (basado en el módulo A) que se establece en el anexo VI; o
	b) procedimiento de examen de tipo UE (basado en el módulo B) que se establece en el anexo VI, seguido de la conformidad de tipo UE basada en el control interno de la producción (basada en el módulo C) que se establece en el anexo VI.

Enmienda 125

Propuesta de Reglamento
Artículo 27 – apartado 5

Texto de la Comisión	*Enmienda*
5. La autoridad notificante preservará la confidencialidad de la información obtenida.	5. La autoridad notificante preservará la confidencialidad de la información obtenida***, incluidos los derechos de propiedad intelectual, la información empresarial confidencial y los secretos comerciales***.

Enmienda 126

Propuesta de Reglamento
Artículo 27 – apartado 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	6 bis. La autoridad notificante reducirá al mínimo la burocracia y las tasas, especialmente para las pymes.

Enmienda 127

Propuesta de Reglamento
Artículo 29 – apartado 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	7 bis. Los Estados miembros y la Comisión adoptarán las medidas apropiadas para garantizar una disponibilidad suficiente de profesionales cualificados, con el fin de reducir al mínimo los cuellos de botella existentes en las actividades de los organismos de evaluación de la conformidad.

Enmienda 128

Propuesta de Reglamento
Artículo 29 – apartado 10

Texto de la Comisión	*Enmienda*
10. El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información recabada en el ejercicio de sus tareas, con arreglo al anexo VI o a cualquier disposición de Derecho interno por la que se aplique, salvo con respecto a las autoridades de vigilancia del mercado del Estado miembro en que realice sus actividades. Se protegerán los derechos de propiedad. El organismo de evaluación de la conformidad contará con procedimientos documentados que garanticen el cumplimiento del presente apartado.	10. El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información recabada en el ejercicio de sus tareas, con arreglo al anexo VI o a cualquier disposición de Derecho interno por la que se aplique, salvo con respecto a las autoridades de vigilancia del mercado del Estado miembro en que realice sus actividades. Se protegerán los derechos de propiedad ***intelectual, la información empresarial confidencial y los secretos comerciales***. El organismo de evaluación de la conformidad contará con procedimientos documentados que garanticen el cumplimiento del presente apartado.

Enmienda 129

Propuesta de Reglamento
Artículo 29 – apartado 12

Texto de la Comisión	*Enmienda*
12. Los organismos de evaluación de la conformidad funcionarán con arreglo a un conjunto de condiciones coherentes, justas y razonables que tengan particularmente en cuenta los intereses de las pymes en relación con las tasas.	12. Los organismos de evaluación de la conformidad funcionarán con arreglo a un conjunto de condiciones coherentes, justas y razonables ***en consonancia con el artículo 37, apartado 2,*** que tengan particularmente en cuenta los intereses ***de las microempresas y*** de las pymes en relación con las tasas.

Enmienda 130

Propuesta de Reglamento
Artículo 36 – apartado 3

Texto de la Comisión	*Enmienda*
3. La Comisión garantizará el tratamiento confidencial de toda la información ***sensible*** recabada en el curso de sus investigaciones.	3. La Comisión garantizará el tratamiento confidencial de toda la información***, incluidos los derechos de propiedad intelectual, la información empresarial confidencial y los secretos comerciales,*** recabada en el curso de sus investigaciones.

Enmienda 131

Propuesta de Reglamento
Artículo 37 – apartado 2

Texto de la Comisión	*Enmienda*
2. Las evaluaciones de la conformidad se llevarán a cabo de manera proporcionada, evitando imponer cargas innecesarias a los operadores económicos. Los organismos de evaluación de la conformidad llevarán a cabo sus actividades teniendo debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura, el grado de complejidad ***de*** la ***tecnología*** del producto	2. Las evaluaciones de la conformidad se llevarán a cabo de manera proporcionada, evitando imponer cargas innecesarias a los operadores económicos***, con una consideración especial para las pymes***. Los organismos de evaluación de la conformidad llevarán a cabo sus actividades teniendo debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura, el grado de

y el carácter masivo o en serie del proceso de producción.	complejidad ***y*** la ***exposición al riesgo*** del ***tipo de*** producto ***y de la tecnología*** y el carácter masivo o en serie del proceso de producción.

Enmienda 132

Propuesta de Reglamento
Artículo 37 – apartado 5

Texto de la Comisión	*Enmienda*
5. Si durante la supervisión de la conformidad posterior a la expedición del certificado, un organismo notificado constata que el producto ya no es conforme con los requisitos establecidos en el presente Reglamento, instará al fabricante a adoptar las medidas correctoras adecuadas y, si es necesario, suspenderá o retirará el certificado.	5. Si durante la supervisión de la conformidad posterior a la expedición del certificado, un organismo notificado constata que el producto ya no es conforme con los requisitos establecidos en el presente Reglamento, instará al fabricante a adoptar las medidas correctoras adecuadas y, si es necesario, ***restringirá,*** suspenderá o retirará el certificado.

Enmienda 133

Propuesta de Reglamento
Artículo 40 – apartado 1

Texto de la Comisión	*Enmienda*
1. La Comisión se asegurará de que se instauren y se gestionen convenientemente una coordinación y una cooperación adecuadas entre los organismos notificados, a través de un grupo intersectorial de organismos notificados.	1. La Comisión se asegurará de que se instauren***, teniendo en cuenta también la necesidad de reducir la burocracia y las tasas,*** y se gestionen convenientemente una coordinación y una cooperación adecuadas entre los organismos notificados, a través de un grupo intersectorial de organismos notificados.

Enmienda 134

Propuesta de Reglamento
Artículo 40 – apartado 2

Texto de la Comisión	*Enmienda*
2. Los Estados miembros se asegurarán de que los organismos notificados por ellos participan en el trabajo de dicho grupo, directamente o por medio de representantes designados.	2. Los Estados miembros se asegurarán de que los organismos notificados por ellos participan en el trabajo de dicho grupo, directamente o por medio de representantes designados***, teniendo en cuenta también la necesidad de reducir la burocracia y las tasas***.

Enmienda 135

Propuesta de Reglamento
Artículo 41 – apartado 3

Texto de la Comisión	*Enmienda*
3. Cuando corresponda, las autoridades de vigilancia del mercado cooperarán con las autoridades nacionales de certificación de la ciberseguridad designadas en virtud del artículo 58 del Reglamento (UE) 2019/881 e intercambiarán información periódicamente. Por lo que respecta a la supervisión de la aplicación de las obligaciones de información con arreglo al artículo 11 del presente Reglamento, las autoridades de vigilancia del mercado designadas cooperarán con la ENISA.	3. Cuando corresponda, las autoridades de vigilancia del mercado cooperarán con las autoridades nacionales de certificación de la ciberseguridad designadas en virtud del artículo 58 del Reglamento (UE) 2019/881 e intercambiarán información periódicamente. Por lo que respecta a la supervisión de la aplicación de las obligaciones de información con arreglo al artículo 11 del presente Reglamento, las autoridades de vigilancia del mercado designadas cooperarán ***eficazmente*** con la ENISA. ***Las autoridades de vigilancia del mercado podrán solicitar a la ENISA que preste asesoramiento técnico sobre asuntos relacionados con la aplicación y la ejecución del presente Reglamento, también durante las investigaciones de conformidad con el artículo 43 cuando las autoridades de vigilancia del mercado puedan solicitar a la ENISA que preste evaluaciones no vinculantes de la conformidad de los productos con elementos digitales.***

Enmienda 136

Propuesta de Reglamento
Artículo 41 – apartado 7

Texto de la Comisión	*Enmienda*
7. La Comisión facilitará el intercambio de experiencias entre las autoridades de vigilancia del mercado designadas.	7. La Comisión facilitará el intercambio ***periódico y estructurado*** de experiencias entre las autoridades de vigilancia del mercado designadas***, entre otras vías, mediante un Grupo de Cooperación Administrativa (ADCO) específico establecido con arreglo al apartado 11 del presente artículo***.

Enmienda 137

Propuesta de Reglamento
Artículo 41 – apartado 8

Texto de la Comisión	*Enmienda*
8. ***Las autoridades de vigilancia del mercado, con el apoyo de la Comisión***, ***podrán proporcionar orientación y asesoramiento a*** los ***operadores económicos*** sobre la aplicación del presente Reglamento.	8. ***La Comisión adoptará directrices y proporcionará asesoramiento a los operadores económicos***, ***en particular a los que cumplan*** los ***requisitos para ser considerados pymes, incluidas las microempresas,*** sobre la aplicación del presente Reglamento. ***En particular, las directrices y el asesoramiento tendrán por objeto simplificar y limitar la carga administrativa y financiera, asegurando al mismo tiempo una aplicación eficaz y coherente de conformidad con el objetivo general de garantizar la seguridad de los productos y la protección de los consumidores.***

Enmienda 138

Propuesta de Reglamento
Artículo 41 – apartado 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	8 bis. Las autoridades de vigilancia del mercado se equiparán para recibir las

reclamaciones formuladas por los consumidores de conformidad con el artículo 11 del Reglamento (UE) 2019/1020 también mediante el establecimiento de un mecanismo claro y accesible que facilite la notificación de vulnerabilidades, incidentes y ciberamenazas.

Enmienda 139

Propuesta de Reglamento
Artículo 41 – apartado 11

Texto de la Comisión	*Enmienda*
11. Se establecerá un Grupo de Cooperación Administrativa (ADCO) específico para la aplicación uniforme del presente Reglamento, de conformidad con el artículo 30, apartado 2, del Reglamento (UE) 2019/1020. Este ADCO estará compuesto por representantes de las autoridades de vigilancia del mercado designadas y, en su caso, por representantes de las oficinas de enlace únicas.	11. Se establecerá un Grupo de Cooperación Administrativa (ADCO) específico para la aplicación uniforme del presente Reglamento***, con el fin de facilitar la cooperación estructurada en relación con la ejecución del presente Reglamento y de optimizar las prácticas de las autoridades de vigilancia del mercado en el seno de la Unión,*** de conformidad con el artículo 30, apartado 2, del Reglamento (UE) 2019/1020. Este ADCO ***se encargará, en particular, de las tareas a que se refiere el artículo 32, apartado 2, del Reglamento (UE) 2019/1020 y*** estará compuesto por representantes de las autoridades de vigilancia del mercado designadas***, la ENISA*** y, en su caso, por representantes de las oficinas de enlace únicas. ***El ADCO se reunirá periódicamente y, cuando sea necesario, previa petición debidamente justificada de la Comisión, de la ENISA, o de un Estado miembro, coordinará su actuación con otras actividades existentes de la Unión relativas a la vigilancia del mercado y la seguridad de los consumidores y, cuando proceda, cooperará e intercambiará información con otras redes, grupos y órganos de la Unión. El ADCO podrá invitar a expertos y otros terceros, incluidas las organizaciones de consumidores, a asistir***

a sus reuniones.

Enmienda 140

Propuesta de Reglamento
Artículo 41 – apartado 11 bis (nuevo)

Texto de la Comisión	*Enmienda*
	11 bis. En el caso de los productos con elementos digitales que entren en el ámbito de aplicación del presente Reglamento, distribuidos, puestos en servicio o utilizados por entidades financieras reguladas por la legislación pertinente de la Unión sobre servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad pertinente responsable de la supervisión financiera de tales entidades con arreglo a dicha legislación.

Enmienda 141

Propuesta de Reglamento
Artículo 42 – párrafo 1

Texto de la Comisión	*Enmienda*
Cuando sea necesario para evaluar la conformidad de los productos con elementos digitales y los procesos establecidos por los fabricantes con los requisitos esenciales establecidos en el anexo I, se concederá a las autoridades de vigilancia del mercado, previa solicitud motivada, acceso a los datos necesarios para evaluar el diseño, el desarrollo y la producción de dichos productos y la gestión de sus vulnerabilidades, incluida la documentación interna correspondiente del operador económico correspondiente.	Cuando sea necesario para evaluar la conformidad de los productos con elementos digitales y los procesos establecidos por los fabricantes con los requisitos esenciales establecidos en el anexo I, se concederá a las autoridades de vigilancia del mercado, previa solicitud motivada, acceso a los datos necesarios para evaluar el diseño, el desarrollo y la producción de dichos productos y la gestión de sus vulnerabilidades, incluida la documentación interna correspondiente del operador económico correspondiente. ***Cuando proceda, y de conformidad con el artículo 52, apartado 1, letra a), tal acceso se efectuará en un entorno seguro y***

controlado determinado por el fabricante.

Enmienda 142

Propuesta de Reglamento
Artículo 43 – apartado 1 – párrafo 2

Texto de la Comisión	*Enmienda*
Si, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado constata que el producto con elementos digitales no cumple los requisitos establecidos en el presente Reglamento, pedirá sin demora al operador pertinente que adopte las medidas correctoras oportunas para llevar el producto a conformidad con los citados requisitos o bien retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo, que dicha autoridad prescriba.	Si, en el transcurso de dicha evaluación, la autoridad de vigilancia del mercado constata que el producto con elementos digitales no cumple los requisitos establecidos en el presente Reglamento ***o constituye de otro modo una amenaza para la seguridad nacional***, pedirá sin demora al operador ***económico*** pertinente que adopte las medidas correctoras oportunas para llevar el producto a conformidad con los citados requisitos o bien retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo, que dicha autoridad prescriba. ***Antes de que se efectúe la evaluación mencionada, en caso necesario, y teniendo en cuenta la relevancia del riesgo de ciberseguridad, la autoridad de vigilancia del mercado podrá exigir al operador de que se trate que suspenda o restrinja de inmediato la disponibilidad del producto en el mercado durante el período de dicha evaluación.***

Enmienda 143

Propuesta de Reglamento
Artículo 43 – apartado 4 – párrafo 1

Texto de la Comisión	*Enmienda*
Si el fabricante de un producto con elementos digitales no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 1, párrafo segundo, la autoridad de vigilancia del	Si el fabricante de un producto con elementos digitales no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 1, párrafo segundo, ***o la autoridad pertinente del***

mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del producto en su mercado nacional, para retirarlo de ese mercado o para recuperarlo.	***Estado miembro considera que el producto representa una amenaza para la seguridad nacional,*** la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del producto en su mercado nacional, para retirarlo de ese mercado o para recuperarlo.

Enmienda 144

Propuesta de Reglamento
Artículo 45 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cuando la Comisión tenga motivos suficientes para considerar, en particular sobre la base de la información facilitada por la ENISA, que un producto con elementos digitales que presenta un riesgo de ciberseguridad significativo no cumple los requisitos establecidos en el presente Reglamento, ***podrá solicitar*** a las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hace referencia el artículo 43.	1. Cuando la Comisión tenga motivos suficientes para considerar, en particular sobre la base de la información facilitada por ***las autoridades competentes de los Estados miembros, los equipos de respuesta a incidentes de seguridad informática (CSIRT) designados o establecidos con arreglo a la Directiva (UE) 2022/2555 o*** la ENISA, que un producto con elementos digitales que presenta un riesgo de ciberseguridad significativo no cumple los requisitos establecidos en el presente Reglamento, ***solicitará*** a las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hace referencia el artículo 43.

Enmienda 145

Propuesta de Reglamento
Artículo 45 – apartado 2

Texto de la Comisión	*Enmienda*
2. En circunstancias ***excepcionales*** que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la	2. En circunstancias que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la Comisión tenga

Comisión tenga motivos ***suficientes*** para considerar que el producto a que hace referencia el apartado 1 sigue sin cumplir los requisitos establecidos en el presente Reglamento y que las autoridades de vigilancia del mercado pertinentes no han adoptado medidas eficaces, la Comisión ***podrá solicitar*** a la ENISA que lleve a cabo una evaluación del cumplimiento. La Comisión informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.

motivos para considerar que el producto a que hace referencia el apartado 1 sigue sin cumplir los requisitos establecidos en el presente Reglamento y que las autoridades de vigilancia del mercado pertinentes no han adoptado medidas eficaces, la Comisión ***solicitará*** a la ENISA que lleve a cabo una evaluación del cumplimiento. La Comisión informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.

Enmienda 146

Propuesta de Reglamento
Artículo 46 – apartado 1

Texto de la Comisión	*Enmienda*
1. Si, tras efectuar una evaluación con arreglo al artículo 43, la autoridad de vigilancia del mercado de un Estado miembro constata que un producto con elementos digitales y los procesos establecidos por el fabricante, a pesar de ser conformes con el presente Reglamento, presentan un riesgo de ciberseguridad significativo y, además, plantean un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones que impone el Derecho nacional o de la Unión en materia de protección de los derechos fundamentales, para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema de información electrónico por entidades esenciales del tipo contemplado en el ***/***anexo I de la Directiva ***XXX/XXXX*** (SRI 2)***/*** o para otros aspectos relativos a la protección del interés público, dicha autoridad exigirá al operador económico pertinente que adopte todas las medidas necesarias para garantizar que el producto con elementos digitales en cuestión y los procesos	1. Si, tras efectuar una evaluación con arreglo al artículo 43, la autoridad de vigilancia del mercado de un Estado miembro constata que un producto con elementos digitales y los procesos establecidos por el fabricante, a pesar de ser conformes con el presente Reglamento, presentan un riesgo de ciberseguridad significativo y, además, plantean un riesgo para la salud o la seguridad de las personas, para el cumplimiento de las obligaciones que impone el Derecho nacional o de la Unión en materia de protección de los derechos fundamentales, para la disponibilidad, autenticidad, integridad o confidencialidad de los servicios ofrecidos mediante un sistema de información electrónico por entidades esenciales del tipo contemplado en el anexo I de la 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***

establecidos por el fabricante ya no presenten ese riesgo cuando se introduzca el producto en el mercado, o bien para retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo.

Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (SRI 2) o para otros aspectos relativos a la protección del interés público, dicha autoridad exigirá al operador económico pertinente que adopte todas las medidas necesarias para garantizar que el producto con elementos digitales en cuestión y los procesos establecidos por el fabricante ya no presenten ese riesgo cuando se introduzca el producto en el mercado, o bien para retirarlo del mercado o recuperarlo en un plazo razonable, proporcional a la naturaleza del riesgo.

Enmienda 147

Propuesta de Reglamento
Artículo 46 – apartado 2

Texto de la Comisión	*Enmienda*
2. El fabricante u otros operadores pertinentes se asegurarán de que se adoptan medidas correctoras con respecto a todos los productos con elementos digitales afectados que hayan comercializado en toda la Unión en el plazo establecido por la autoridad de vigilancia del mercado del Estado miembro a que hace referencia el apartado 1.	2. El fabricante u otros operadores ***económicos*** pertinentes se asegurarán de que se adoptan medidas correctoras con respecto a todos los productos con elementos digitales afectados que hayan comercializado en toda la Unión en el plazo establecido por la autoridad de vigilancia del mercado del Estado miembro a que hace referencia el apartado 1.

Enmienda 148

Propuesta de Reglamento
Artículo 46 – apartado 6

Texto de la Comisión	*Enmienda*
6. Cuando la Comisión tenga motivos suficientes para considerar, en particular sobre la base de la información facilitada por la ENISA, que un producto con elementos digitales, a pesar de ser conforme con el presente Reglamento, presenta los riesgos a que hace referencia	6. Cuando la Comisión tenga motivos suficientes para considerar, en particular sobre la base de la información facilitada por la ENISA, que un producto con elementos digitales, a pesar de ser conforme con el presente Reglamento, presenta los riesgos a que hace referencia

el apartado 1, ***podrá solicitar*** a la autoridad o las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hacen referencia el artículo 43 y los apartados 1, 2 y 3 del presente artículo.

el apartado 1, ***solicitará*** a la autoridad o las autoridades de vigilancia del mercado pertinentes que lleven a cabo una evaluación del cumplimiento y sigan los procedimientos a que hacen referencia el artículo 43 y los apartados 1, 2 y 3 del presente artículo.

Enmienda 149

Propuesta de Reglamento
Artículo 46 – apartado 7

Texto de la Comisión	*Enmienda*
7. En circunstancias ***excepcionales*** que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto a que hace referencia el apartado 6 sigue presentando los riesgos a que hace referencia el apartado 1 y que las autoridades de vigilancia del mercado nacionales pertinentes no han adoptado medidas eficaces, la Comisión ***podrá solicitar*** a la ENISA que lleve a cabo una evaluación de los riesgos que presenta el producto e informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.	7. En circunstancias que justifiquen una intervención inmediata para preservar el buen funcionamiento del mercado interior y siempre que la Comisión tenga motivos suficientes para considerar que el producto a que hace referencia el apartado 6 sigue presentando los riesgos a que hace referencia el apartado 1 y que las autoridades de vigilancia del mercado nacionales pertinentes no han adoptado medidas eficaces, la Comisión ***solicitará*** a la ENISA que lleve a cabo una evaluación de los riesgos que presenta el producto e informará de ello a las autoridades de vigilancia del mercado pertinentes. Los operadores económicos pertinentes cooperarán con la ENISA en todo lo necesario.

Enmienda 150

Propuesta de Reglamento
Artículo 48 – apartado 1

Texto de la Comisión	*Enmienda*
1. Las autoridades de vigilancia del mercado ***podrán acordar*** con otras autoridades pertinentes ***la realización de actividades conjuntas*** con objeto de	1. Las autoridades de vigilancia del mercado ***realizarán periódicamente actividades conjuntas*** con otras autoridades pertinentes con objeto de

garantizar la ciberseguridad y la protección de los consumidores respecto de productos específicos con elementos digitales introducidos en el mercado o comercializados, en particular aquellos que con frecuencia presentan riesgos de ciberseguridad.	garantizar la ciberseguridad y la protección de los consumidores respecto de productos específicos con elementos digitales introducidos en el mercado o comercializados, en particular aquellos que con frecuencia presentan riesgos de ciberseguridad. ***Tales actividades incluirán la inspección de productos adquiridos bajo una identidad encubierta.***

Enmienda 151

Propuesta de Reglamento
Artículo 48 – apartado 2

Texto de la Comisión	*Enmienda*
2. La Comisión o la ENISA ***podrán proponer*** actividades conjuntas de control del cumplimiento del presente Reglamento que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre posibles incumplimientos en varios Estados miembros de los requisitos establecidos por el presente Reglamento por parte de los productos que entran en el ámbito de aplicación de este.	2. La Comisión o la ENISA ***propondrán*** actividades conjuntas de control del cumplimiento del presente Reglamento que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre posibles incumplimientos en varios Estados miembros de los requisitos establecidos por el presente Reglamento por parte de los productos que entran en el ámbito de aplicación de este.

Enmienda 152

Propuesta de Reglamento
Artículo 49 – apartado 1

Texto de la Comisión	*Enmienda*
1. Las autoridades de vigilancia del mercado ***podrán llevar*** a cabo acciones de control simultáneas coordinadas («barridos») de determinados productos con elementos digitales o categorías de estos para comprobar el cumplimiento o detectar infracciones del presente Reglamento.	1. Las autoridades de vigilancia del mercado ***llevarán periódicamente*** a cabo acciones de control simultáneas coordinadas («barridos») de determinados productos con elementos digitales o categorías de estos para comprobar el cumplimiento o detectar infracciones del presente Reglamento.

Enmienda 153

Propuesta de Reglamento
Artículo 49 – apartado 2

Texto de la Comisión	*Enmienda*
2. Salvo que las autoridades de vigilancia del mercado implicadas acuerden otra cosa, los barridos serán coordinados por la Comisión. El coordinador del barrido ***podrá***, en su caso, ***hacer públicos*** los resultados agregados.	2. Salvo que las autoridades de vigilancia del mercado implicadas acuerden otra cosa, los barridos serán coordinados por la Comisión. El coordinador del barrido ***hará públicos***, en su caso, los resultados agregados.

Enmienda 154

Propuesta de Reglamento
Artículo 49 – apartado 3

Texto de la Comisión	*Enmienda*
3. En el desempeño de sus funciones, la ENISA ***podrá determinar***, en particular sobre la base de las notificaciones recibidas de conformidad con el artículo 11, apartados 1 y 2, categorías de productos para las que ***puedan organizarse*** barridos. La propuesta de barrido se presentará al posible coordinador mencionado en el apartado 2 para su examen por las autoridades de vigilancia del mercado.	3. En el desempeño de sus funciones, la ENISA ***determinará***, en particular sobre la base de las notificaciones recibidas de conformidad con el artículo 11, apartados 1 y 2, categorías de productos para las que ***se organizarán*** barridos. La propuesta de barrido se presentará al posible coordinador mencionado en el apartado 2 para su examen por las autoridades de vigilancia del mercado.

Enmienda 155

Propuesta de Reglamento
Artículo 49 – apartado 5

Texto de la Comisión	*Enmienda*
5. Las autoridades de vigilancia del mercado ***podrán invitar*** a funcionarios de la Comisión y otros acompañantes autorizados por esta a participar en las operaciones de barrido.	5. Las autoridades de vigilancia del mercado ***invitarán*** a funcionarios de la Comisión y otros acompañantes autorizados por esta a participar en las operaciones de barrido.

Enmienda 156

Propuesta de Reglamento
Artículo 49 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 49 bis
	Prestación de asesoramiento técnico
	1. La Comisión, mediante un acto de ejecución, designará un grupo de expertos para que preste asesoramiento técnico a las autoridades de vigilancia del mercado sobre asuntos relacionados con la aplicación y la ejecución del presente Reglamento. El acto de ejecución especificará, entre otros aspectos, los detalles de la composición del grupo, su funcionamiento y la remuneración de sus miembros. En particular, el grupo de expertos llevará a cabo evaluaciones no vinculantes de productos con elementos digitales previa petición al respecto de una autoridad de vigilancia del mercado que lleve a cabo una investigación con arreglo al artículo 43, y de la lista de productos críticos con elementos digitales establecida en el anexo II, así como sobre la posible necesidad de actualizar dicha lista.
	2. El grupo constará de expertos independientes designados para un mandato renovable de tres años por la Comisión con arreglo a su pericia científica o técnica en el ámbito considerado.
	3. La Comisión designará un número de expertos que considere suficiente para atender las necesidades previstas.
	4. La Comisión adoptará las medidas necesarias para gestionar y evitar conflictos de intereses. Las declaraciones de intereses de los miembros del grupo de expertos se pondrán a disposición del público.
	5. Los expertos designados llevarán a

cabo sus tareas con el máximo nivel de profesionalismo, independencia, imparcialidad y objetividad.

6. Al adoptar posiciones, puntos de vista e informes, el grupo de expertos procurará alcanzar consensos. Si no pueden alcanzarse, las decisiones se tomarán por mayoría simple de los miembros del grupo.

Enmienda 157

Propuesta de Reglamento
Artículo 53 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros establecerán las normas sobre las sanciones aplicables a las infracciones del presente Reglamento cometidas por los operadores económicos y adoptarán todas las medidas necesarias para garantizar su ejecución. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias.	1. Los Estados miembros establecerán las normas sobre las sanciones aplicables a las infracciones del presente Reglamento cometidas por los operadores económicos y adoptarán todas las medidas necesarias para garantizar su ejecución. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias***, y tendrán en cuenta las especificidades de las microempresas y de las pequeñas y medianas empresas***.

Enmienda 158

Propuesta de Reglamento
Artículo 53 – apartado 6 – letra a bis (nueva)

Texto de la Comisión	*Enmienda*
	a bis) si la infracción no es intencionada;

Enmienda 159

Propuesta de Reglamento
Artículo 53 – apartado 6 – letra b

Texto de la Comisión	*Enmienda*
b) si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por una infracción similar;	b) si ***las mismas u*** otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por una infracción similar;

Enmienda 160

Propuesta de Reglamento
Artículo 53 – apartado 6 – letra c

Texto de la Comisión	*Enmienda*
c) el tamaño y la cuota de mercado del operador que comete la infracción**.**	c) el tamaño y la cuota de mercado del operador que comete la infracción***, teniendo en cuenta la escala de los riesgos, las consecuencias y las especificidades financieras de las microempresas y las pequeñas y medianas empresas;***

Enmienda 161

Propuesta de Reglamento
Artículo 53 – apartado 6 – letra c bis (nueva)

Texto de la Comisión	*Enmienda*
	c bis) el comportamiento del operador al adquirir información o conocimiento del incumplimiento en cuestión, también si, al conocer el incumplimiento en cuestión, el operador empleó todas las medidas correctivas apropiadas, así como las medidas razonablemente necesarias, para evitar o reducir al mínimo las posibles consecuencias negativas.

Enmienda 162

Propuesta de Reglamento
Capítulo VII bis (nuevo)

Texto de la Comisión	*Enmienda*
	MEDIDAS DE APOYO A LA INNOVACIÓN

Enmienda 163

Propuesta de Reglamento
Artículo 53 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 53 bis
	Espacios controlados de pruebas
	La Comisión y la ENISA podrán establecer un espacio controlado de pruebas europeo con la participación voluntaria de los fabricantes de productos con elementos digitales con el fin de:
	a) proporcionar un entorno controlado que facilite el desarrollo, la comprobación y la validación del diseño, el desarrollo y la producción de productos con elementos digitales antes de su comercialización o su puesta en servicio con arreglo a un plan específico;
	b) prestar asistencia práctica a los operadores económicos, entre otras vías, mediante orientaciones y buenas prácticas para cumplir los requisitos esenciales establecidos en el anexo I;
	c) contribuir a un aprendizaje reglamentario basado en pruebas.

Enmienda 164

Propuesta de Reglamento
Artículo 54 – título

Texto de la Comisión	*Enmienda*
Modificación del Reglamento (UE) 2019/1020	Modificación del Reglamento (UE) 2019/1020 ***y de la Directiva (UE)***

2020/1828

Enmienda 165

Propuesta de Reglamento
Artículo 54 – párrafo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. En el anexo I de la Directiva (UE) 2020/1828 se añade el punto siguiente:
	«67) [Reglamento XXX] [Ley de Ciberresiliencia]».

Enmienda 166

Propuesta de Reglamento
Artículo 54 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 54 bis
	Reglamento Delegado (UE) 2022/30
	El presente Reglamento se ha diseñado de manera que todos los productos sujetos a los requisitos esenciales formulados en el artículo 3, apartado 3, letras d), e) y f), de la Directiva 2014/53/UE conforme se describe en el Reglamento Delegado (UE) 2022/30 se atengan al presente Reglamento. Con el fin de generar seguridad jurídica, el Reglamento Delegado (UE) 2022/30 se derogará cuando el presente Reglamento entre en vigor.

Enmienda 167

Propuesta de Reglamento
Artículo 57 – párrafo 2

Texto de la Comisión	*Enmienda*
Será aplicable a partir del [***veinticuatro***	Será aplicable a partir del [***treinta y seis***

meses después de la fecha de entrada en vigor del presente Reglamento]. ***No obstante***, ***el artículo 11 será aplicable a partir del [doce*** meses después de la fecha de ***entrada en vigor*** del presente Reglamento].	meses después de la fecha de entrada en vigor del presente Reglamento]. ***Por lo que se refiere a los productos con elementos críticos***, ***los capítulos II, III, V y VII serán aplicables una vez transcurridos [veinte*** meses después de la fecha de ***publicación de las normas armonizadas desarrolladas con arreglo a la petición de normalización a efectos*** del presente Reglamento]. ***A más tardar seis meses después de la fecha de entrada en vigor del presente Reglamento, la Comisión publicará directrices sobre la manera de aplicar los requisitos formulados en el presente Reglamento a los productos intangibles.***

Enmienda 168

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – parte introductoria

Texto de la Comisión	*Enmienda*
3) Sobre la base de la evaluación de riesgos a la que hace referencia el artículo 10, apartado 2, y cuando proceda, los productos con elementos digitales:	3) Sobre la base de la evaluación de riesgos ***para la ciberseguridad*** a la que hace referencia el artículo 10, apartado 2, y cuando proceda, los productos con elementos digitales:

Enmienda 169

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra –a (nueva)

Texto de la Comisión	*Enmienda*
	–a) se comercializarán sin vulnerabilidades conocidas que puedan aprovecharse respecto a un dispositivo externo o una red;

Enmienda 170

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra a

Texto de la Comisión	*Enmienda*
a) se entregarán con una configuración segura por defecto***, que incluya la posibilidad de restablecer el producto a su estado original***;	a) se entregarán con una configuración segura por defecto;

Enmienda 171

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra c

Texto de la Comisión	*Enmienda*
c) protegerán la confidencialidad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, mediante, por ejemplo, el cifrado de los datos en reposo o en tránsito pertinentes por medio de los mecanismos más avanzados;	c) protegerán la confidencialidad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, mediante, por ejemplo, el cifrado***, la toquenización, los controles de compensación u otros medios de protección adecuados*** de los datos en reposo o en tránsito pertinentes por medio de los mecanismos más avanzados;

Enmienda 172

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra d

Texto de la Comisión	*Enmienda*
d) protegerán la integridad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, los comandos, los programas y la configuración frente a toda manipulación o modificación no autorizada por el usuario, e informarán sobre los casos de corrupción de datos;	d) protegerán la integridad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, los comandos, los programas y la configuración frente a toda manipulación o modificación no autorizada por el usuario, e informarán sobre los casos de corrupción de datos ***o de posibles casos de acceso no autorizado***;

Enmienda 173

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra f

Texto de la Comisión	*Enmienda*
f) protegerán la disponibilidad de funciones esenciales, incluida la resiliencia frente a ataques de denegación de servicio y la mitigación de sus efectos;	f) protegerán la disponibilidad de funciones esenciales ***y básicas***, incluida la resiliencia frente a ataques de denegación de servicio y la mitigación de sus efectos;

Enmienda 174

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra i

Texto de la Comisión	*Enmienda*
i) estarán diseñados, desarrollados y producidos para reducir el impacto de un incidente, por medio de mecanismos y técnicas adecuados para paliar el aprovechamiento de las vulnerabilidades;	i) estarán diseñados, desarrollados y producidos para reducir el impacto de un incidente ***significativo***, por medio de mecanismos y técnicas adecuados para paliar el aprovechamiento de las vulnerabilidades;

Enmienda 175

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra j

Texto de la Comisión	*Enmienda*
j) proporcionarán información relacionada con la seguridad mediante el registro o el seguimiento de la actividad interna pertinente, incluidos el acceso a datos, servicios o funciones y la modificación de estos;	j) proporcionarán información relacionada con la seguridad mediante ***la provisión a petición de los usuarios de capacidades para*** el registro o el seguimiento***, a escala local o del dispositivo,*** de la actividad interna pertinente, incluidos el acceso a datos, servicios o funciones y la modificación de estos;

Enmienda 176

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra k

Texto de la Comisión	*Enmienda*
k) garantizarán que las vulnerabilidades puedan subsanarse mediante actualizaciones de seguridad, incluidas, cuando proceda, las actualizaciones automáticas y la notificación de las actualizaciones disponibles a los usuarios**.**	k) garantizarán que las vulnerabilidades puedan subsanarse mediante actualizaciones de seguridad ***separadas de las actualizaciones de funcionalidad***, incluidas, cuando proceda, las actualizaciones automáticas y la notificación de las actualizaciones disponibles a los usuarios***;***

Enmienda 177

Propuesta de Reglamento
Anexo I – parte 1 – punto 3 – letra k bis (nueva)

Texto de la Comisión	*Enmienda*
	k bis) se diseñarán, desarrollarán y producirán para permitir su supresión segura y el posible reciclaje cuando alcancen el final de su ciclo de vida útil, entre otras vías, permitiendo a los usuarios que supriman y retiren de manera segura todos los datos con carácter permanente.

Enmienda 178

Propuesta de Reglamento
Anexo I – parte 2 – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
2) por lo que respecta a los riesgos para los productos con elementos digitales, abordarán y subsanarán las vulnerabilidades sin demora, en particular mediante la provisión de actualizaciones de seguridad;	2) por lo que respecta a los riesgos para los productos con elementos digitales, abordarán y subsanarán las vulnerabilidades ***críticas y graves*** sin demora, en particular mediante la provisión de actualizaciones de seguridad***, o documentarán los motivos para no subsanar la vulnerabilidad***;

Enmienda 179

Propuesta de Reglamento
Anexo I – parte 2 – párrafo 1 – punto 4

Texto de la Comisión	*Enmienda*
4) una vez esté disponible una actualización de seguridad, divulgarán información sobre las vulnerabilidades subsanadas, incluidas una descripción de las vulnerabilidades, información que permita a los usuarios identificar el producto con elementos digitales afectado, las repercusiones y la gravedad de las vulnerabilidades e información que ayude a los usuarios a corregir las vulnerabilidades;	4) una vez esté disponible una actualización de seguridad, divulgarán ***públicamente o con arreglo a las buenas prácticas del sector*** información sobre las vulnerabilidades ***conocidas*** subsanadas, incluidas una descripción de las vulnerabilidades, información que permita a los usuarios identificar el producto con elementos digitales afectado, las repercusiones y la gravedad de las vulnerabilidades e información ***clara y accesible*** que ayude a los usuarios a corregir las vulnerabilidades;

Enmienda 180

Propuesta de Reglamento
Anexo I – parte 2 – párrafo 1 – punto 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis) la información relativa a las subsanaciones y las vulnerabilidades se compartirá y divulgará de un modo controlado, respetando los principios de «reducción de daños» y los secretos comerciales mediante la divulgación responsable de las vulnerabilidades a los agentes que puedan actuar para mitigar la vulnerabilidad, y no se pondrá a disposición del público a fin de evitar el riesgo de informar de manera inadvertida a posibles atacantes;

Enmienda 181

Propuesta de Reglamento
Anexo I – parte 2 – párrafo 1 – punto 7

Texto de la Comisión	*Enmienda*
7) preverán mecanismos para distribuir de manera segura las actualizaciones de los productos con elementos digitales, con el fin de garantizar que las vulnerabilidades aprovechables se subsanen o se mitiguen de manera oportuna;	7) preverán mecanismos para distribuir de manera segura las actualizaciones ***de seguridad*** de los productos con elementos digitales, con el fin de garantizar que las vulnerabilidades aprovechables se subsanen o se mitiguen de manera oportuna;

Enmienda 182

Propuesta de Reglamento
Anexo I – parte 2 – párrafo 1 – punto 8

Texto de la Comisión	*Enmienda*
8) garantizarán que, cuando ***se disponga de*** parches o actualizaciones de seguridad para hacer frente a los problemas de seguridad detectados, estos se difundan sin demora y de forma gratuita, acompañados de mensajes de aviso que proporcionen a los usuarios la información pertinente, en particular en relación con las posibles medidas que deban adoptarse.	8) garantizarán que, cuando ***puedan facilitarse razonablemente*** parches o actualizaciones de seguridad para hacer frente a los problemas de seguridad detectados, ***existan medios a través de los cuales los usuarios puedan obtenerlos y*** estos se difundan sin demora y de forma gratuita ***o a un coste transparente y no discriminatorio***, acompañados de mensajes de aviso que proporcionen a los usuarios la información pertinente, en particular en relación con las posibles medidas que deban adoptarse.

Enmienda 183

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
2. el punto de contacto en el que pueda notificarse y obtenerse información sobre las vulnerabilidades de ciberseguridad del producto;	2. el punto de contacto ***único*** en el que pueda notificarse y obtenerse información sobre las vulnerabilidades de ciberseguridad del producto;

Enmienda 184

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 5

Texto de la Comisión	*Enmienda*
5. cualquier circunstancia conocida o previsible, asociada al uso del producto con elementos digitales conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos de ciberseguridad significativos;	***suprimido***

Enmienda 185

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 6

Texto de la Comisión	*Enmienda*
6. si ***se puede*** acceder a la nomenclatura de materiales de los programas informáticos y, en su caso, dónde se puede acceder a ella;	6. si ***las autoridades competentes pueden*** acceder a la nomenclatura de materiales de los programas informáticos y, en su caso, dónde se puede acceder a ella;

Enmienda 186

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 8

Texto de la Comisión	*Enmienda*
8. el tipo de apoyo técnico en materia de seguridad ofrecido por el fabricante y hasta cuándo se prestará dicho servicio ***o, al menos, hasta cuándo está previsto que los usuarios puedan recibir actualizaciones de seguridad***;	8. el tipo de apoyo técnico en materia de seguridad ofrecido por el fabricante y hasta cuándo se prestará dicho servicio;

Enmienda 187

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	8 bis. la fecha final de la vida útil prevista del producto, mostrando claramente, en su caso, en el embalaje del producto, hasta cuándo garantizará el fabricante la gestión efectiva de las vulnerabilidades y la provisión de actualizaciones de seguridad;

Enmienda 188

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 9 – letra a

Texto de la Comisión	*Enmienda*
a) las medidas necesarias durante la puesta en servicio inicial y a lo largo de toda la vida del producto para garantizar su uso seguro;	***suprimida***

Enmienda 189

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 9 – letra b

Texto de la Comisión	*Enmienda*
b) cómo los cambios en el producto pueden afectar a la seguridad de los datos;	***suprimida***

Enmienda 190

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 9 – letra c bis (nueva)

Texto de la Comisión	*Enmienda*
	c bis) la vida útil prevista del producto y hasta cuándo garantiza el fabricante la gestión efectiva de vulnerabilidades y la provisión de actualizaciones de seguridad;

Enmienda 191

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 9 – letra d

Texto de la Comisión	*Enmienda*
d) cómo realizar la retirada del servicio del producto de forma segura, incluida información sobre cómo pueden eliminarse de forma segura los datos de los usuarios.	***suprimida***

Enmienda 192

Propuesta de Reglamento
Anexo III – clase I – punto 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. Plataformas de autenticación, autorización y contabilidad (AAC);

Enmienda 193

Propuesta de Reglamento
Anexo III – clase I – punto 15

Texto de la Comisión	*Enmienda*
15. Interfaces físicas de red;	15. Interfaces físicas ***y virtuales*** de red;

Enmienda 194

Propuesta de Reglamento
Anexo III – clase I – punto 18

Texto de la Comisión	*Enmienda*
18. Encaminadores, módems destinados a la conexión a internet e interruptores, no incluidos en la clase II;	***suprimido***

Enmienda 195

Propuesta de Reglamento
Anexo III – clase I – punto 23

Texto de la Comisión	*Enmienda*
23. Internet ***industrial*** de las cosas no incluido en la clase II.	23. ***productos industriales con elementos digitales a los que es posible referirse como parte del*** internet de las cosas no incluido en la clase II.

Enmienda 196

Propuesta de Reglamento
Anexo III – clase II – punto 4

Texto de la Comisión	*Enmienda*
4. Cortafuegos y sistemas de detección o prevención de intrusiones destinados a un uso industrial;	4. Cortafuegos***, pasarelas de seguridad*** y sistemas de detección o prevención de intrusiones destinados a un uso industrial;

Enmienda 197

Propuesta de Reglamento
Anexo III – clase II – punto 7

Texto de la Comisión	*Enmienda*
7. Encaminadores, módems destinados a la conexión a internet ***e*** interruptores ***destinados a un uso industrial***;	7. Encaminadores, módems destinados a la conexión a internet***,*** interruptores***, y otros nodos de red que son necesarios para la provisión del servicio de conectividad***;

Enmienda 198

Propuesta de Reglamento
Anexo IV bis (nuevo)

Texto de la Comisión	*Enmienda*
	ANEXO IV bis

	DECLARACIÓN UE DE INCORPORACIÓN PARA PRODUCTOS PARCIALMENTE COMPLETADOS CON ELEMENTOS DIGITALES
	La declaración UE de incorporación para productos parcialmente completados con elementos digitales a que hace referencia el artículo 20 bis contendrá toda la información siguiente:
	1. El nombre y el tipo del producto parcialmente completado con elementos digitales, y toda información adicional que permita su identificación única;
	2. El objeto de la declaración (identificación del producto parcialmente completado que permita la trazabilidad. Podrá incluir, cuando proceda, una fotografía);
	3. La afirmación de que el producto parcialmente completado descrito anteriormente es conforme a la legislación de armonización de la Unión pertinente;
	4. Referencias a cualquier acto pertinente de la Unión de que se trate, incluidas las referencias de publicación;
	5. Información adicional:
	Firmado por y en nombre de:
	……
	(lugar y fecha de expedición):
	(nombre, cargo) (firma):

Enmienda 199

Propuesta de Reglamento
Anexo V – párrafo 1 – punto 1 – letra a

Texto de la Comisión	*Enmienda*
a) su finalidad prevista;	***suprimida***

Enmienda 200

Propuesta de Reglamento
Anexo V – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
2. una descripción del diseño, el desarrollo y la producción del producto y de los procesos de gestión de las vulnerabilidades, que incluya:	***suprimido***
a) información completa sobre el diseño y el desarrollo del producto con elementos digitales, incluidos, en su caso, planos y esquemas, o una descripción de la arquitectura del sistema que explique cómo se apoyan o se alimentan mutuamente los componentes de los programas informáticos y cómo se integran en el tratamiento general;	
b) información completa y especificaciones de los procesos de gestión de las vulnerabilidades establecidos por el fabricante, incluida la nomenclatura de materiales de los programas informáticos, la política de divulgación coordinada de vulnerabilidades, pruebas de que se ha facilitado una dirección de contacto para la notificación de vulnerabilidades y una descripción de las soluciones técnicas elegidas para la distribución segura de las actualizaciones;	
c) información completa y especificaciones de los procesos de producción y seguimiento del producto con elementos digitales y la validación de estos procesos;	

Enmienda 201

Propuesta de Reglamento
Anexo V – párrafo 1 – punto 3

Texto de la Comisión	*Enmienda*
3. una evaluación de los riesgos de ciberseguridad frente a los cuales se haya	3. ***una declaración o resumen de los riesgos de ciberseguridad frente a los***

diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, tal como se establece en el artículo 10 del presente Reglamento;	***cuales se haya diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, tal como se establece en el artículo 10 del presente Reglamento y, previa petición justificada formulada por una autoridad de vigilancia del mercado, a condición de que sea necesaria para que esta autoridad pueda comprobar el cumplimiento de los requisitos esenciales formulados en el anexo I,*** una evaluación ***detallada*** de los riesgos de ciberseguridad frente a los cuales se haya diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, tal como se establece en el artículo 10 del presente Reglamento;

ANEXO: LISTA DE LAS ORGANIZACIONES O PERSONAS QUE HAN COLABORADO CON EL PONENTE DE OPINIÓN

La lista siguiente se elabora con carácter totalmente voluntario y bajo la exclusiva responsabilidad del ponente de opinión. Las siguientes organizaciones o personas han colaborado con el ponente de opinión durante la preparación del proyecto de opinión:

Organización o persona
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

Título	Requisitos horizontales de ciberseguridad para los productos con elementos digitales y modificación del Reglamento (UE) 2019/1020
Referencias	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Comisión competente para el fondo Fecha del anuncio en el Pleno	ITRE 9.11.2022
Opinión emitida por Fecha del anuncio en el Pleno	IMCO 9.11.2022
Comisiones asociadas - Fecha del anuncio en el Pleno	20.4.2023
Ponente de opinión Fecha de designación	Morten Løkkegaard 16.12.2022
Examen en comisión	2.3.2023 25.4.2023 23.5.2023
Fecha de aprobación	29.6.2023
Resultado de la votación final	+: 41 –: 1 0: 0
Miembros presentes en la votación final	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoş, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann
Suplentes presentes en la votación final	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski
Suplentes (art. 209, apdo. 7) presentes en la votación final	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski

VOTACIÓN FINAL NOMINAL
EN LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

Explicación de los signos utilizados
+ : a favor
- : en contra
0 : abstenciones