



2017/0225(COD)

1.2.2018

PROYECTO DE 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 ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)
(COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Ponente de opinión: (*) Nicola Danti

(*) Procedimiento de comisiones asociadas — artículo 54 del Reglamento interno

PA_Legam

BREVE JUSTIFICACIÓN

En la era digital, la ciberseguridad constituye un elemento básico de la competitividad económica y la seguridad de la Unión Europea, y de la integridad de nuestras sociedades libres y democráticas y los procesos que las sustentan. Garantizar un alto grado de ciberresiliencia en toda la UE reviste una importancia fundamental de cara a concitar la confianza de los consumidores en el mercado único digital y a seguir desarrollando una Europa más innovadora y competitiva.

Sin lugar a dudas, las ciberamenazas y los ciberataques a nivel mundial—como «WannaCry» y «Meltdown»— son problemas de importancia creciente en nuestra cada vez más digitalizada sociedad. Según una encuesta del Eurobarómetro publicada en julio de 2017, el 87 % de los encuestados opinan que la ciberdelincuencia representa un notable desafío para la seguridad interior de la UE, y una mayoría de ellos están preocupados por ser víctimas de diversas formas de ciberdelincuencia. Por otra parte, desde comienzos de 2016 se han producido cada día en todo el mundo más de 4 000 ataques de *ransom-ware* (bloqueo de archivos con petición de un rescate), lo que supone un aumento del 300 % respecto a 2015, afectando al 80 % de las empresas de la UE. Estos hechos y conclusiones ponen claramente de manifiesto la necesidad de que la UE sea más resiliente y eficaz a la hora de luchar contra los ciberataques e incremente su capacidad para proteger mejor a los ciudadanos, las empresas y las instituciones públicas de la Unión.

Un año después de la entrada en vigor de la Directiva SRI, la Comisión Europea, en el marco más amplio de la estrategia de ciberseguridad de la UE, presentó un Reglamento que tiene por objeto aumentar la resiliencia, la disuasión y la defensa cibernética de la UE. El 13 de septiembre de 2017, la Comisión presentó el «Reglamento de Ciberseguridad», basado en dos pilares:

1) un mandato reforzado para la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) al objeto de ayudar a los Estados miembros a prevenir y responder eficazmente a los ciberataques, y 2) la creación de un marco de la UE para la certificación de la ciberseguridad que garantice la ciberseguridad de los productos y servicios de TIC.

En general, el ponente acoge con satisfacción el enfoque propuesto por la Comisión Europea y, en particular, se muestra favorable a la introducción de regímenes de certificación de la ciberseguridad a escala de la UE, que pretenden aumentar la seguridad de los productos y servicios de TIC y evitar la costosa fragmentación del mercado único en este ámbito crucial. Aunque inicialmente debe seguir siendo un instrumento voluntario, el ponente espera que un marco de la UE para la certificación de la ciberseguridad y los procedimientos correspondientes se conviertan en un instrumento necesario para reforzar la confianza de los ciudadanos y usuarios e incrementar la seguridad de los productos y servicios que circulan en el mercado único.

Ciertamente, está convencido asimismo de que hay una serie de puntos de la propuesta que deben clarificarse y mejorarse:

- En primer lugar, **el aumento de la participación de las partes interesadas relevantes en las distintas fases del sistema de gobernanza de cara a la preparación de propuestas de regímenes de certificación por ENISA:** en opinión del ponente, es fundamental implicar oficialmente a las partes interesadas más relevantes, como las empresas del sector de las TIC, las organizaciones de consumidores, las pymes, las organizaciones europeas de normalización y las agencias sectoriales de la UE, entre otras, y darles la posibilidad de plantear nuevas propuestas

de regímenes, asesorar a ENISA con sus conocimientos específicos o cooperar con ENISA en la preparación de una propuesta de régimen.

- En segundo lugar, es necesario reforzar el papel de coordinación del Grupo Europeo de Certificación de la Ciberseguridad (compuesto por autoridades nacionales, con el apoyo de la Comisión y de ENISA) con las tareas adicionales de proporcionar orientación estratégica y **elaborar un programa de trabajo sobre las acciones comunes que deben llevarse a cabo a nivel de la Unión** en el ámbito de la certificación, así como de establecer y **actualizar periódicamente una lista prioritaria de los productos y servicios de TIC** para los que considera que se precisa un régimen europeo de certificación de la ciberseguridad.
- El ponente cree firmemente que debemos evitar la práctica del «shopping» (compra) de la certificación de la UE, como ya ha ocurrido en otros sectores. Las **disposiciones de control y vigilancia de ENISA y las autoridades nacionales de supervisión de la certificación deben ser firmemente reforzadas** a fin de garantizar que un certificado europeo expedido en un Estado miembro obedezca a las mismas normas y requisitos que uno expedido en otro Estado miembro. Por tanto, propone:
 - 1) reforzar las competencias de vigilancia de ENISA: junto con el Grupo de Certificación, ENISA debe efectuar evaluaciones de los procedimientos aplicados por las autoridades competentes en materia de expedición de los certificados de la UE;
 - 2) que las autoridades nacionales de supervisión de la certificación deban llevar a cabo evaluaciones periódicas (al menos cada dos años) de los certificados de la UE emitidos por los organismos de evaluación de la conformidad;
 - 3) introducir criterios vinculantes comunes definidos por el Grupo con miras a establecer la escala, el alcance y la frecuencia con que las autoridades nacionales de supervisión de la certificación deban realizar las evaluaciones a que se hace referencia en el punto 2.
- El ponente considera que debe introducirse una **etiqueta de confianza de la UE** obligatoria para los productos y servicios de TIC destinados a los usuarios finales. Esta etiqueta podría contribuir a elevar la concienciación sobre la ciberseguridad y dar a las empresas con buenas credenciales de ciberseguridad una ventaja competitiva.
- El ponente está de acuerdo con el enfoque uniforme y armonizado adoptado por la Comisión, pero está convencido de que debe ser más flexible y adaptable a las características y vulnerabilidades específicas de cada producto o servicio, y no responder a un planteamiento de «solución única». Por consiguiente, el ponente considera que los **niveles de seguridad** deben ser renombrados y utilizados teniendo en cuenta también el uso previsto de los productos y servicios de TIC. Igualmente, la duración de la **validez del certificado** debe fijarse en cada régimen de manera específica.
- Cada régimen de certificación debe diseñarse de modo que estimule y anime a todos los actores implicados del sector de que se trate a desarrollar y adoptar normas de seguridad, normas técnicas y **principios de seguridad a través del diseño y de**

intimidad a través del diseño en todas las fases del ciclo de vida del producto o servicio.

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 5

Texto de la Comisión

(5) A la luz de los crecientes retos que tiene planteados la Unión en materia de ciberseguridad, es necesario un conjunto completo de medidas que se apoye en actuaciones previas de la Unión y promueva objetivos que se refuercen mutuamente. Entre ellas se incluye la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación y la coordinación en los Estados miembros y las instituciones, órganos y organismos de la UE. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades a nivel de la Unión que podrían complementar la acción de los Estados miembros, en particular en caso de ciberincidentes y crisis transfronterizas a gran escala. Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones de ciberseguridad. Además, debe reforzarse la confianza en el mercado único digital ofreciendo información transparente sobre el nivel de seguridad de los productos y servicios de TIC. Esto puede verse facilitado por una certificación a escala de la UE que aporte requisitos y criterios de evaluación de la ciberseguridad comunes en todos los mercados y sectores nacionales.

Enmienda

(5) A la luz de los crecientes retos que tiene planteados la Unión en materia de ciberseguridad, es necesario un conjunto completo de medidas que se apoye en actuaciones previas de la Unión y promueva objetivos que se refuercen mutuamente. Entre ellas se incluye la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación y la coordinación en los Estados miembros y las instituciones, órganos y organismos de la UE. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades a nivel de la Unión que podrían complementar la acción de los Estados miembros, en particular en caso de ciberincidentes y crisis transfronterizas a gran escala. Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones de ciberseguridad. Además, ***dado que los ciberincidentes socavan la confianza en los proveedores de servicios digitales y en el mercado único digital en sí, especialmente entre los consumidores,*** debe reforzarse la confianza ofreciendo información transparente sobre el nivel de seguridad de los productos y servicios de TIC. Esto puede verse facilitado por una certificación a escala de la UE que aporte requisitos y criterios de evaluación de la

ciberseguridad comunes en todos los mercados y sectores nacionales. ***Junto con una certificación a escala de la Unión, existe una serie de medidas voluntarias que el sector privado debería adoptar para reforzar la confianza en la seguridad de los productos y servicios de TIC, en particular en vista de la creciente disponibilidad de dispositivos de la internet de las cosas. Por ejemplo, deberían utilizarse de forma más eficaz el cifrado y otras tecnologías, como la tecnología de cadena de bloques, con el fin de mejorar la seguridad de las comunicaciones y los datos de los usuarios finales y la seguridad global de las redes y los sistemas de información en la Unión.***

Or. en

Enmienda 2

Propuesta de Reglamento Considerando 7

Texto de la Comisión

(7) La Unión ha adoptado ya medidas importantes para garantizar la ciberseguridad y aumentar la confianza en las tecnologías digitales. En 2013, se adoptó una Estrategia de ciberseguridad de la UE para orientar la respuesta política de la Unión a las amenazas y riesgos relacionados con la ciberseguridad. En su esfuerzo por proteger mejor a los europeos en línea, la Unión adoptó en 2016 el primer acto legislativo en el ámbito de la ciberseguridad, la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en lo sucesivo, «Directiva SRI»). La Directiva SRI instauró requisitos relativos a las capacidades nacionales en el ámbito de la

Enmienda

(7) La Unión ha adoptado ya medidas importantes para garantizar la ciberseguridad y aumentar la confianza en las tecnologías digitales. En 2013, se adoptó una Estrategia de ciberseguridad de la UE para orientar la respuesta política de la Unión a las amenazas y riesgos relacionados con la ciberseguridad. En su esfuerzo por proteger mejor a los europeos en línea, la Unión adoptó en 2016 el primer acto legislativo en el ámbito de la ciberseguridad, la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en lo sucesivo, «Directiva SRI»). La Directiva SRI, ***cuyo éxito dependerá fundamentalmente de su eficaz puesta en***

ciberseguridad, estableció los primeros mecanismos para mejorar la cooperación estratégica y operativa entre los Estados miembros e introdujo obligaciones relativas a medidas de seguridad y notificaciones de incidentes en todos los sectores fundamentales para la economía y la sociedad, como la energía, los transportes, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad, las infraestructuras digitales, así como los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea). Se atribuyó un papel clave a ENISA para respaldar la aplicación de esta Directiva. Además, una lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, contribuyendo al objetivo general de conseguir un elevado nivel de ciberseguridad.

marcha por parte de los Estados miembros, instauró requisitos relativos a las capacidades nacionales en el ámbito de la ciberseguridad, estableció los primeros mecanismos para mejorar la cooperación estratégica y operativa entre los Estados miembros e introdujo obligaciones relativas a medidas de seguridad y notificaciones de incidentes en todos los sectores fundamentales para la economía y la sociedad, como la energía, los transportes, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad, las infraestructuras digitales, así como los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea). Se atribuyó un papel clave a ENISA para respaldar la aplicación de esta Directiva. Además, una lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, contribuyendo al objetivo general de conseguir un elevado nivel de ciberseguridad.

Or. en

Enmienda 3

Propuesta de Reglamento Considerando 28

Texto de la Comisión

(28) La Agencia debe contribuir a la sensibilización del público sobre los riesgos para la ciberseguridad y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos y organizaciones. Debe contribuir asimismo a promover las mejores prácticas y soluciones a nivel de personas y organizaciones mediante la recogida y análisis de la información disponible públicamente relativa a

Enmienda

(28) La Agencia debe contribuir a la sensibilización del público sobre los riesgos para la ciberseguridad y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos y organizaciones. Debe contribuir asimismo a promover las mejores prácticas y soluciones a nivel de personas y organizaciones mediante la recogida y análisis de la información disponible públicamente relativa a

incidentes significativos y la elaboración de informes con vistas a ofrecer orientaciones a empresas y ciudadanos y mejorar el nivel general de preparación y resiliencia. La Agencia debe además, en colaboración con los Estados miembros y las instituciones, órganos y organismos de la Unión, organizar campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y a concienciar sobre las amenazas potenciales en el ciberespacio, incluyendo ciberdelitos como los ataques por suplantación de identidad (phishing), las redes infectadas (botnets) o los fraudes bancarios y financieros, así como dar consejos básicos en materia de autenticación y protección de datos. La Agencia debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos.

incidentes significativos y la elaboración de informes con vistas a ofrecer orientaciones a empresas y ciudadanos y mejorar el nivel general de preparación y resiliencia. La Agencia debe además, en colaboración con los Estados miembros y las instituciones, órganos y organismos de la Unión, organizar campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y a concienciar sobre las amenazas potenciales en el ciberespacio, incluyendo ciberdelitos como los ataques por suplantación de identidad (phishing), las redes infectadas (botnets) o los fraudes bancarios y financieros, así como dar consejos básicos en materia de autenticación, protección de datos, ***cifrado y otras tecnologías de mejora de la seguridad y la intimidad y herramientas de anonimización***. La Agencia debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos.

Or. en

Enmienda 4

Propuesta de Reglamento Considerando 36 bis (nuevo)

Texto de la Comisión

Enmienda

(36 bis) Las normas son una herramienta voluntaria guiada por el mercado que proporciona requisitos técnicos y orientaciones y que se deriva de un proceso abierto, transparente e integrador. El uso de normas facilita que los bienes y servicios cumplan el Derecho de la Unión y respalda las políticas europeas en consonancia con el Reglamento (UE) n.º 1025/2012 sobre la normalización europea. La Agencia debe

consultar y trabajar de forma regular en cooperación con las organizaciones europeas de normalización, en particular a la hora de preparar los regímenes europeos de certificación de la ciberseguridad.

Or. en

Enmienda 5

Propuesta de Reglamento Considerando 44

Texto de la Comisión

(44) La Agencia debe contar con un Grupo Permanente de Partes Interesadas en calidad de organismo consultivo, a fin de garantizar un diálogo sistemático con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes. El Grupo Permanente de Partes Interesadas, establecido por el Consejo de Administración a propuesta del director ejecutivo, debe centrarse en cuestiones que afecten a las partes interesadas y ponerlas en conocimiento de la Agencia. La composición del Grupo Permanente de Partes Interesadas y las tareas asignadas a este grupo, que debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo, deben garantizar una representación suficiente de las partes interesadas en los trabajos de la Agencia.

Enmienda

(44) La Agencia debe contar con un Grupo Permanente de Partes Interesadas en calidad de organismo consultivo, a fin de garantizar un diálogo sistemático con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes. El Grupo Permanente de Partes Interesadas, establecido por el Consejo de Administración a propuesta del director ejecutivo, debe centrarse en cuestiones que afecten a las partes interesadas y ponerlas en conocimiento de la Agencia. ***A fin de garantizar una participación oportuna de las partes interesadas en el marco de certificación de la ciberseguridad, el Grupo Permanente de Partes Interesadas debe asimismo asesorar sobre qué productos y servicios de TIC han de incluirse en los regímenes europeos de certificación de la ciberseguridad, y proponer a la Comisión que solicite a la Agencia que prepare propuestas de regímenes sobre dichos productos y servicios de TIC.*** La composición del Grupo Permanente de Partes Interesadas y las tareas asignadas a este grupo, que debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo, deben garantizar una representación suficiente de las partes interesadas en los trabajos de la Agencia.

Enmienda 6**Propuesta de Reglamento****Considerando 52***Texto de la Comisión*

(52) Por todo ello, es necesario establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar regímenes europeos de certificación de la ciberseguridad y permita que los certificados de productos y servicios de TIC sean reconocidos y usados en todos los Estados miembros. El marco europeo debe tener un doble objetivo: por una parte, contribuir a aumentar la confianza en los productos y servicios de TIC que hayan sido certificados con arreglo a tales regímenes; por otra, evitar la multiplicación de certificaciones nacionales de la ciberseguridad contradictorias o redundantes y, por ende, reducir los costes para las empresas que operan en el mercado único digital. Los regímenes deben ser no discriminatorios y basarse en normas internacionales o de la Unión, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la UE al respecto.

Enmienda

(52) Por todo ello, es necesario establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar regímenes europeos de certificación de la ciberseguridad y permita que los certificados de productos y servicios de TIC sean reconocidos y usados en todos los Estados miembros. ***A este respecto, es esencial aprovechar los regímenes nacionales e internacionales existentes, así como los sistemas de reconocimiento mutuo, en particular el SOG-IS, y hacer posible una transición sin problemas de los regímenes existentes bajo dichos sistemas a los regímenes en virtud del nuevo marco europeo.*** El marco europeo debe tener un doble objetivo: por una parte, contribuir a aumentar la confianza en los productos y servicios de TIC que hayan sido certificados con arreglo a tales regímenes; por otra, evitar la multiplicación de certificaciones nacionales de la ciberseguridad contradictorias o redundantes y, por ende, reducir los costes para las empresas que operan en el mercado único digital. Los regímenes deben ser no discriminatorios y basarse en normas internacionales o de la Unión, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la UE al respecto.

Enmienda 7

Propuesta de Reglamento Considerando 55

Texto de la Comisión

(55) El objetivo de los regímenes europeos de certificación de la ciberseguridad debe ser garantizar que los productos y servicios de TIC certificados con arreglo a un régimen cumplan los requisitos especificados. Tales requisitos se refieren a la capacidad de resistir, con un nivel determinado de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, procesos, servicios y sistemas, en el sentido del presente Reglamento, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle en el presente Reglamento los requisitos de ciberseguridad relativos a todos los productos y servicios de TIC. Los productos y servicios de TIC y las correspondientes necesidades de ciberseguridad son tan dispares que es muy difícil presentar unos requisitos de ciberseguridad generales de validez global. Por lo tanto, es necesario adoptar un concepto amplio y general de la ciberseguridad a efectos de la certificación, complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los regímenes europeos de certificación de la ciberseguridad. Las modalidades con que se lograrán tales objetivos para determinados productos y servicios de TIC deben especificarse luego con más detalle a nivel de cada régimen de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas.

Enmienda

(55) El objetivo de los regímenes europeos de certificación de la ciberseguridad debe ser garantizar que los productos y servicios de TIC certificados con arreglo a un régimen cumplan los requisitos especificados. Tales requisitos se refieren a la capacidad de resistir, con un nivel determinado de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, procesos, servicios y sistemas, en el sentido del presente Reglamento, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle en el presente Reglamento los requisitos de ciberseguridad relativos a todos los productos y servicios de TIC. Los productos y servicios de TIC y las correspondientes necesidades de ciberseguridad son tan dispares que es muy difícil presentar unos requisitos de ciberseguridad generales de validez global. Por lo tanto, es necesario adoptar un concepto amplio y general de la ciberseguridad a efectos de la certificación, complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los regímenes europeos de certificación de la ciberseguridad. Las modalidades con que se lograrán tales objetivos para determinados productos y servicios de TIC deben especificarse luego con más detalle a nivel de cada régimen de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas. ***Reviste una importancia crucial que cada régimen europeo de certificación de la***

ciberseguridad se diseñe de modo que estimule y anime a todos los actores implicados del sector de que se trate a desarrollar y adoptar normas de seguridad, normas técnicas y principios de seguridad a través del diseño y de intimidad a través del diseño en todas las fases del ciclo de vida del producto o servicio.

Or. en

Enmienda 8

Propuesta de Reglamento Considerando 56

Texto de la Comisión

(56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. A continuación, la Comisión, sobre la base de las propuestas presentadas por ENISA, debe estar facultada para adoptar el régimen europeo de certificación de la ciberseguridad mediante actos de ejecución. Teniendo en cuenta la finalidad general y los objetivos de seguridad definidos en el presente Reglamento, los regímenes europeos de certificación de la ciberseguridad adoptados por la Comisión deben especificar un conjunto mínimo de elementos relacionados con el objeto, alcance y funcionamiento del régimen concreto. Entre ellos deben figurar el alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos y servicios de TIC que cubre, la especificación detallada de los requisitos de ciberseguridad, por ejemplo haciendo referencia a normas o especificaciones técnicas, los criterios y métodos de evaluación específicos, así como el nivel de garantía: *básico, sustancial o elevado*.

Enmienda

(56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. A continuación, la Comisión, sobre la base de las propuestas presentadas por ENISA, debe estar facultada para adoptar el régimen europeo de certificación de la ciberseguridad mediante actos de ejecución. ***Con el fin de reforzar la confianza y previsibilidad y elevar la sensibilización de los ciudadanos en lo que se refiere al marco de certificación de la ciberseguridad, ENISA debe mantener un sitio web específico con una herramienta en línea fácil de usar que recoja información sobre los regímenes adoptados, las propuestas de regímenes y los regímenes solicitados por la Comisión.*** Teniendo en cuenta la finalidad general y los objetivos de seguridad definidos en el presente Reglamento, los regímenes europeos de certificación de la ciberseguridad adoptados por la Comisión deben especificar un conjunto mínimo de elementos relacionados con el objeto, alcance y funcionamiento del régimen concreto. Entre ellos deben figurar el

alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos y servicios de TIC que cubre, la especificación detallada de los requisitos de ciberseguridad, por ejemplo haciendo referencia a normas o especificaciones técnicas, los criterios y métodos de evaluación específicos *asociados al funcionamiento y el uso de un producto, proceso o servicio de TIC*, así como el nivel de garantía: *seguro, sustancialmente seguro, extremadamente seguro, o cualquier combinación de ellos. Un elemento valioso que debe incluirse en los regímenes de certificación es el uso de marcas o etiquetas que indiquen un cierto nivel de ciberseguridad, especialmente para los productos y servicios de TIC destinados a usuarios finales. Tales marcas o etiquetas contribuirían a elevar la sensibilización acerca de las cuestiones de ciberseguridad entre los consumidores y a prepararles para elegir con conocimiento de causa, ofreciéndoles información clara y comprensible sobre los productos y servicios de TIC, también en relación con las actualizaciones de software, y a dar a las empresas con buenas credenciales de ciberseguridad una ventaja competitiva. Dicha etiqueta podría tener la forma de un logotipo digital o un código QR y proporcionaría calificaciones de ciberseguridad o indicaría los riesgos asociados con el funcionamiento y la utilización de un dispositivo de la internet de los objetos, sobre la base de los requisitos establecidos en la Directiva SRI. A fin de fomentar el uso de marcas o etiquetas, la Comisión debería proponer la introducción de una etiqueta de confianza de la Unión para los productos y servicios de TIC destinados a usuarios finales.*

Or. en

Enmienda 9

Propuesta de Reglamento Considerando 59

Texto de la Comisión

(59) Es necesario exigir a todos los Estados miembros que designen a una autoridad de supervisión de la certificación de la ciberseguridad para supervisar el cumplimiento, por parte de los organismos de evaluación de la conformidad establecidos en su territorio y de los certificados por ellos expedidos, de los requisitos del presente Reglamento y de los regímenes de certificación de la ciberseguridad pertinentes. Las autoridades nacionales de supervisión de la certificación deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigar el asunto objeto de la reclamación en la medida que proceda e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable. Además, deben cooperar con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes de ciberseguridad específicos.

Enmienda

(59) Es necesario exigir a todos los Estados miembros que designen a una autoridad de supervisión de la certificación de la ciberseguridad para supervisar el cumplimiento, por parte de los organismos de evaluación de la conformidad establecidos en su territorio y de los certificados por ellos expedidos, de los requisitos del presente Reglamento y de los regímenes de certificación de la ciberseguridad pertinentes. Las autoridades nacionales de supervisión de la certificación deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigar el asunto objeto de la reclamación en la medida que proceda e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable. Además, deben cooperar con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes de ciberseguridad específicos. ***La cooperación eficaz entre las autoridades nacionales de supervisión de la certificación es esencial para la correcta aplicación de los regímenes europeos de certificación de la ciberseguridad y de cuestiones técnicas en relación con la ciberseguridad de los productos y servicios de TIC. La Comisión debe facilitar ese intercambio de información mediante la puesta a disposición de un sistema general de apoyo a la información electrónica, por***

ejemplo, el sistema de información y comunicación para la vigilancia del mercado (ICSMS) y el sistema de alerta rápida para productos peligrosos no alimenticios (RAPEX), ya utilizados por las autoridades de vigilancia del mercado en virtud de lo dispuesto en el Reglamento (CE) n.º 765/2008.

Or. en

Enmienda 10

Propuesta de Reglamento Considerando 63

Texto de la Comisión

Enmienda

(63) A fin de precisar los criterios para la acreditación de los organismos de evaluación de la conformidad, deben delegarse en la Comisión los poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. La Comisión debe llevar a cabo las oportunas consultas durante sus trabajos preparatorios, también a nivel de expertos. Dichas consultas deben realizarse de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016. En particular, para garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

suprimido

Or. en

Enmienda 11

Propuesta de Reglamento Considerando 65

Texto de la Comisión

(65) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, sobre las modalidades de ejecución de las investigaciones por parte de la Agencia y sobre las circunstancias, formatos y procedimientos de notificación a la Comisión por parte de los organismos de evaluación de la conformidad acreditados por las autoridades nacionales de supervisión de la certificación.

Enmienda

(65) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, sobre las modalidades de ejecución de las investigaciones por parte de la Agencia y sobre las circunstancias, formatos y procedimientos de notificación a la Comisión por parte de los organismos de evaluación de la conformidad acreditados por las autoridades nacionales de supervisión de la certificación, ***teniendo en cuenta la probada eficacia de la herramienta de notificación electrónica denominada «Sistema de información sobre organismos notificados y designados de nuevo enfoque» (NANDO).***

Or. en

Enmienda 12

Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 11

Texto de la Comisión

11) «producto y servicio de TIC», ***todo elemento o grupo de elementos*** de las redes y los sistemas de información;

Enmienda

11) «producto y servicio de TIC», ***un producto, servicio, proceso, sistema o combinación de los anteriores que sea un elemento*** de las redes y los sistemas de información;

Or. en

Enmienda 13

Propuesta de Reglamento

Artículo 2 – párrafo 1 – punto 11 bis (nuevo)

Texto de la Comisión

Enmienda

(11 bis) «autoridad nacional de supervisión de la certificación», una autoridad de un Estado miembro responsable de la ejecución de tareas de control, cumplimiento y supervisión en relación con la certificación de la ciberseguridad en su territorio;

Or. en

Justificación

Conviene incluir una definición de esta entidad.

Enmienda 14

Propuesta de Reglamento

Artículo 3 – apartado 1

Texto de la Comisión

Enmienda

1. La Agencia desempeñará los cometidos que le asigna el presente Reglamento con el fin de contribuir a un elevado nivel de ciberseguridad dentro de la Unión.

1. La Agencia desempeñará los cometidos que le asigna el presente Reglamento con el fin de contribuir *al logro de* un elevado nivel *común* de ciberseguridad dentro de la Unión, *reducir la fragmentación en el mercado interior y mejorar su funcionamiento.*

Or. en

Enmienda 15

Propuesta de Reglamento

Artículo 4 – apartado 5

Texto de la Comisión

Enmienda

5. La Agencia *incrementará* las

5. La Agencia *contribuirá a*

capacidades de ciberseguridad a nivel de la Unión para complementar la acción de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

incrementar las capacidades de ciberseguridad a nivel de la Unión para complementar **y reforzar** la acción de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

Or. en

Enmienda 16

Propuesta de Reglamento Artículo 4 – apartado 6

Texto de la Comisión

6. La Agencia promoverá el uso de la certificación, **en particular contribuyendo** a la creación y el mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.

Enmienda

6. La Agencia promoverá el uso de la certificación **y la normalización, evitando al mismo tiempo la fragmentación ocasionada por la falta de coordinación entre los regímenes de certificación existentes en la Unión. La Agencia contribuirá** a la creación y el mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.

Or. en

Enmienda 17

Propuesta de Reglamento Artículo 8 – párrafo 1 – letra a – punto 1 bis (nuevo)

Texto de la Comisión

Enmienda

1 bis) realizar, en cooperación con el Grupo Europeo de Certificación de la Ciberseguridad, evaluaciones de los

procedimientos de expedición de los certificados europeos de ciberseguridad puestos en marcha por los organismos de evaluación de la conformidad a que se refiere el artículo 51, cuyo objeto es garantizar la aplicación uniforme del presente Reglamento por parte de los organismos de evaluación de la conformidad en lo que se refiere a la expedición de certificados;

Or. en

Enmienda 18

Propuesta de Reglamento

Artículo 8 – párrafo 1 – letra b

Texto de la Comisión

b) Facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos y servicios de TIC y elaborará, en colaboración con los Estados miembros, directrices y orientaciones relativas a las áreas técnicas relacionadas con los requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, así como relativas a normas ya existentes, entre ellas las normas nacionales de los Estados miembros, con arreglo al artículo 19, apartado 2, de la Directiva (UE) 2016/1148.

Enmienda

b) ***Consultará a las organizaciones europeas de normalización acerca de la evolución de las normas europeas, velará por la idoneidad de las normas utilizadas en los regímenes de certificación aprobados*** y facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos y servicios de TIC y elaborará, en colaboración con los Estados miembros, directrices y orientaciones relativas a las áreas técnicas relacionadas con los requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, así como relativas a normas ya existentes, entre ellas las normas nacionales de los Estados miembros, con arreglo al artículo 19, apartado 2, de la Directiva (UE) 2016/1148.

Or. en

Enmienda 19

Propuesta de Reglamento Artículo 20 – apartado 1

Texto de la Comisión

1. El Consejo de Administración establecerá, a propuesta del director ejecutivo, un Grupo Permanente de Partes Interesadas integrado por expertos reconocidos que representen a las partes interesadas pertinentes, tales como la industria de las TIC, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, los grupos de consumidores, expertos académicos en ciberseguridad y representantes de las autoridades competentes notificadas con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas] y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos.

Enmienda

1. El Consejo de Administración establecerá, a propuesta del director ejecutivo, un Grupo Permanente de Partes Interesadas integrado por expertos reconocidos que representen a las partes interesadas pertinentes, tales como la industria de las TIC, **las asociaciones de pymes**, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, los grupos **y las asociaciones** de consumidores, expertos académicos en **el ámbito de la** ciberseguridad, **las organizaciones europeas de normalización, según se definen en el punto 8 del artículo 2 del Reglamento (UE) n.º 1025/2012, los órganos y organismos sectoriales de la Unión competentes**, y representantes de las autoridades competentes notificadas con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas] y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos.

Or. en

Justificación

Es importante garantizar que el Grupo Permanente de Partes Interesadas se compone de todas las partes interesadas.

Enmienda 20

Propuesta de Reglamento Artículo 20 – apartado 5

Texto de la Comisión

5. El Grupo Permanente de Partes Interesadas asesorará a la Agencia en lo

Enmienda

5. El Grupo Permanente de Partes Interesadas asesorará a la Agencia en lo

relativo a la realización de sus actividades. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo de la Agencia y en el mantenimiento de la comunicación con las partes interesadas pertinentes sobre todos los aspectos relativos al programa de trabajo.

relativo a la realización de sus actividades. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo de la Agencia y en el mantenimiento de la comunicación con las partes interesadas pertinentes sobre todos los aspectos relativos al programa de trabajo. ***Podrá asimismo proponer que la Comisión solicite a la Agencia que prepare propuestas de regímenes europeos de certificación de la ciberseguridad de conformidad con el artículo 44.***

Or. en

Justificación

Vinculada al artículo 44, apartado 1. Habida cuenta de los conocimientos disponibles en la composición ampliada del Grupo Permanente de Partes Interesadas, es conveniente que tenga también la facultad de proponer regímenes de certificación.

Enmienda 21

Propuesta de Reglamento Artículo 44 – apartado 1

Texto de la Comisión

1. Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de certificación de la ciberseguridad que cumpla los requisitos expuestos en los artículos 45, 46 y 47 del presente Reglamento. Los Estados miembros **o** el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») establecido de conformidad con el artículo 53 podrán proponer a la Comisión la preparación de un régimen europeo de certificación de la ciberseguridad.

Enmienda

1. Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de certificación de la ciberseguridad que cumpla los requisitos expuestos en los artículos 45, 46 y 47 del presente Reglamento. Los Estados miembros, el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») establecido de conformidad con el artículo 53 **o el Grupo Permanente de Partes Interesadas** podrán proponer a la Comisión la preparación de un régimen europeo de certificación de la ciberseguridad.

Or. en

Justificación

Véase la justificación del artículo 20, apartado 5.

Enmienda 22

Propuesta de Reglamento Artículo 44 – apartado 2

Texto de la Comisión

2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ENISA consultará a todas las partes interesadas y cooperará estrechamente con el Grupo. El Grupo facilitará a ENISA la asistencia y el asesoramiento experto que requiera en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes en caso necesario.

Enmienda

2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ENISA consultará **al Grupo Permanente de Partes Interesadas, en particular a las organizaciones europeas de normalización**, y a todas las partes interesadas **restantes** y cooperará estrechamente con el Grupo. El Grupo facilitará a ENISA la asistencia y el asesoramiento experto que requiera en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes en caso necesario.

Cuando proceda, ENISA podrá crear asimismo un grupo de expertos de las partes interesadas compuesto por miembros del Grupo Permanente de Partes Interesadas y cualesquiera otras partes interesadas pertinentes con experiencia específica en el ámbito de una determinada propuesta de régimen, a fin de prestar una mayor asistencia y asesoramiento.

Or. en

Justificación

Dado que existe el Grupo Permanente de Partes Interesadas, debería ser mencionado aquí con derechos de consulta. Las organizaciones europeas de normalización desempeñarán un papel crucial en el procedimiento de certificación, de modo que ENISA debería estar obligada a cooperar estrechamente con ellas. Asimismo, como la gama de productos y servicios de TIC que podrían estar sujetos a un régimen es muy amplia, la creación de grupos de expertos con conocimientos específicos en el ámbito de una determinada propuesta de régimen sería una buena manera de garantizar la adecuada preparación del régimen.

Enmienda 23

Propuesta de Reglamento Artículo 44 – apartado 5

Texto de la Comisión

5. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los regímenes europeos de certificación de la ciberseguridad y darles publicidad.

Enmienda

5. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los regímenes europeos de certificación de la ciberseguridad y darles publicidad, ***incluida la información sobre todas las propuestas de régimen que la Comisión haya solicitado a ENISA que prepare.***

Or. en

Justificación

En aras de la transparencia y la previsibilidad, el sitio web debe incluir no solo información sobre regímenes finalizados, sino también sobre todos los regímenes que la Comisión haya solicitado a ENISA que prepare.

Enmienda 24

Propuesta de Reglamento Artículo 45 – párrafo 1 – parte introductoria

Texto de la Comisión

Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, ***según proceda***, los siguientes objetivos de seguridad:

Enmienda

Todos los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, ***al menos***, los siguientes objetivos de seguridad:

Or. en

Enmienda 25

Propuesta de Reglamento Artículo 45 – párrafo 1 – letra g

Texto de la Comisión

g) garantizar que los productos y servicios de TIC se entreguen siempre con un software actualizado, que no contenga vulnerabilidades conocidas, y dispongan de mecanismos para efectuar actualizaciones de seguridad del software.

Enmienda

g) garantizar que los productos y servicios de TIC se entreguen siempre con un software y **hardware** actualizado, que no contenga vulnerabilidades conocidas, y dispongan de mecanismos para efectuar actualizaciones de seguridad del software y **del hardware, incluidas las actualizaciones automáticas de seguridad.**

Or. en

Enmienda 26

Propuesta de Reglamento

Artículo 45 – párrafo 1 – letra g bis (nueva)

Texto de la Comisión

Enmienda

g bis) garantizar que los productos y servicios de TIC se desarrollan según el principio de «seguridad a través del diseño».

Or. en

Justificación

Es de la máxima importancia que todos los actores de la cadena de valor aseguren la ciberseguridad sus productos y servicios de una forma dinámica desde la fase más temprana del proceso de ingeniería.

Enmienda 27

Propuesta de Reglamento

Artículo 46 – apartado 1

Texto de la Comisión

Enmienda

1. **Un** régimen europeo de certificación de la ciberseguridad podrá especificar uno o más de los siguientes niveles de garantía: **básico, sustancial y/o elevado**, para los productos y servicios de

1. **Todo** régimen europeo de certificación de la ciberseguridad podrá especificar uno o más de los siguientes niveles de garantía: **«funcionalmente seguro», «sustancialmente seguro» y/o**

TIC amparados en dicho régimen.

«*extremadamente seguro*», para los productos y servicios de TIC amparados en dicho régimen, *teniendo en cuenta, entre otros factores, el uso previsto de los mismos*.

Or. en

Justificación

El nivel de garantía de cada régimen de certificación de la ciberseguridad debe tener en cuenta el uso o el destino de los productos y servicios de TIC, y no los productos y servicios de TIC en sí.

Enmienda 28

Propuesta de Reglamento

Artículo 46 – apartado 2 – parte introductoria

Texto de la Comisión

2. Los niveles de garantía *básico*, *sustancial* y *elevado* cumplirán los siguientes criterios, respectivamente:

Enmienda

2. Los niveles de garantía «*funcionalmente seguro*», «*sustancialmente seguro*» y «*extremadamente seguro*» cumplirán los siguientes criterios, respectivamente:

Or. en

Enmienda 29

Propuesta de Reglamento

Artículo 46 – apartado 2 – letra a

Texto de la Comisión

a) el nivel de garantía *bajo* se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado *limitado* de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos,

Enmienda

a) el nivel de garantía «*funcionalmente seguro*» se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado *adecuado* de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos

cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;

conexos, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;

Or. en

Enmienda 30

Propuesta de Reglamento Artículo 46 – apartado 2 – letra b

Texto de la Comisión

b) el nivel de garantía *sustancial* se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado sustancial de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir sustancialmente el riesgo de incidentes de ciberseguridad;

Enmienda

b) el nivel de garantía «*sustancialmente seguro*» se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado sustancial de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir sustancialmente el riesgo de incidentes de ciberseguridad;

Or. en

Enmienda 31

Propuesta de Reglamento Artículo 46 – apartado 2 – letra c

Texto de la Comisión

c) el nivel de garantía *elevado* se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC superior al de los certificados con nivel de garantía *sustancial*, y se

Enmienda

c) el nivel de garantía «*extremadamente seguro*» se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC superior al de los certificados con nivel de garantía

caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.

«*sustancialmente seguro*», y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.

Or. en

Enmienda 32

Propuesta de Reglamento

Artículo 47 – apartado 1 – parte introductoria

Texto de la Comisión

1. *Un* régimen europeo de certificación de la ciberseguridad incluirá los siguientes elementos:

Enmienda

1. *Todo* régimen europeo de certificación de la ciberseguridad incluirá, *al menos*, los siguientes elementos:

Or. en

Enmienda 33

Propuesta de Reglamento

Artículo 47 – apartado 1 – letra f

Texto de la Comisión

f) cuando el régimen prevea marcas o etiquetas, las condiciones en las que pueden utilizarse tales marcas o etiquetas;

Enmienda

f) cuando el régimen prevea marcas o etiquetas, *como la etiqueta de confianza de la UE*, las condiciones en las que pueden utilizarse tales marcas o etiquetas; *todos los regímenes que cubran productos o servicios de TIC destinados a usuarios finales dispondrán de marcas o etiquetas;*

Or. en

Justificación

Debería elaborarse una etiqueta de confianza de la UE con el fin de ayudar a los usuarios finales a elegir con conocimiento de causa y a aumentar la sensibilización del público sobre las cuestiones relacionadas con la ciberseguridad.

Enmienda 34

Propuesta de Reglamento

Artículo 47 – apartado 1 – letra g

Texto de la Comisión

g) **cuando la vigilancia forme parte del régimen**, las normas para controlar el cumplimiento de los requisitos de los certificados, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

Enmienda

g) las normas para controlar el cumplimiento de los requisitos de los certificados, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

Or. en

Justificación

La vigilancia debe ser un elemento central en todo régimen.

Enmienda 35

Propuesta de Reglamento

Artículo 47 – apartado 1 – letra h

Texto de la Comisión

h) condiciones para la concesión, el mantenimiento, la continuación, la ampliación y la reducción del alcance de la certificación;

Enmienda

h) condiciones para la concesión, el mantenimiento, la continuación, **la renovación**, la ampliación y la reducción del alcance de la certificación;

Or. en

Enmienda 36

Propuesta de Reglamento

Artículo 47 – apartado 1 – letra l

Texto de la Comisión

l) identificación de los regímenes nacionales de certificación de la

Enmienda

l) identificación de los regímenes nacionales **e internacionales** de

ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC;

certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC;

Or. en

Enmienda 37

Propuesta de Reglamento

Artículo 47 – apartado 1 – letra m bis (nueva)

Texto de la Comisión

Enmienda

m bis) período máximo de validez de los certificados, si procede.

Or. en

Justificación

Vinculada a la enmienda al artículo 48, apartado 6.

Enmienda 38

Propuesta de Reglamento

Artículo 48 – apartado 4 – parte introductoria

Texto de la Comisión

Enmienda

4. No obstante lo dispuesto en el apartado 3, en casos debidamente justificados un régimen europeo de ciberseguridad particular podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese régimen. Este organismo público será uno de los siguientes:

4. No obstante lo dispuesto en el apartado 3, en casos debidamente justificados, **como por motivos de seguridad nacional**, un régimen europeo de ciberseguridad particular podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese régimen. Este organismo público será uno de los siguientes:

Or. en

Enmienda 39

Propuesta de Reglamento Artículo 48 – apartado 5

Texto de la Comisión

5. La persona física o jurídica que presenta sus productos o servicios de TIC al mecanismo de certificación facilitará al organismo de evaluación de la conformidad a que se refiere el artículo 51 toda la información necesaria para llevar a cabo el procedimiento de certificación.

Enmienda

5. La persona física o jurídica que presenta sus productos o servicios de TIC al mecanismo de certificación facilitará al organismo de evaluación de la conformidad a que se refiere el artículo 51 toda la información necesaria para llevar a cabo el procedimiento de certificación, ***incluida la información sobre toda vulnerabilidad o riesgo de seguridad conocidos.***

Or. en

Enmienda 40

Propuesta de Reglamento Artículo 48 – apartado 6

Texto de la Comisión

6. Los certificados se expedirán por ***un*** período ***máximo de tres años*** y podrán renovarse en las mismas condiciones, siempre y cuando sigan cumpliéndose los requisitos correspondientes.

Enmienda

6. Los certificados se expedirán por ***el*** período ***que se fije en cada régimen de certificación*** y podrán renovarse en las mismas condiciones, siempre y cuando sigan cumpliéndose los requisitos correspondientes.

Or. en

Justificación

Dada la amplia y variada gama de productos y servicios de TIC para los que podrían desarrollarse regímenes, parece arbitrario establecer un período máximo de validez en el presente Reglamento.

Enmienda 41

Propuesta de Reglamento Artículo 50 – apartado 6 – letra a

Texto de la Comisión

a) controlarán e impondrán la aplicación de las disposiciones del presente título a nivel nacional y **supervisarán** la conformidad de los certificados que hayan sido emitidos por los organismos de evaluación de la conformidad establecidos en sus territorios respectivos con los requisitos establecidos en el presente título y en el correspondiente régimen europeo de certificación de la ciberseguridad;

Enmienda

a) controlarán e impondrán la aplicación de las disposiciones del presente título a nivel nacional y **verificarán** la conformidad de los certificados que hayan sido emitidos por los organismos de evaluación de la conformidad establecidos en sus territorios respectivos con los requisitos establecidos en el presente título y en el correspondiente régimen europeo de certificación de la ciberseguridad, **de conformidad con las normas adoptadas por el Grupo Europeo de Certificación de la Ciberseguridad en virtud de la letra d bis) del apartado 3 del artículo 53;**

Or. en

Justificación

Las disposiciones de control y vigilancia de las autoridades nacionales de supervisión de la certificación han de reforzarse notablemente de cara a evitar la práctica del «shopping» (compra) de la certificación de la UE. Con arreglo a esta disposición, las autoridades nacionales de supervisión de la certificación han de verificar la conformidad de un número de certificados emitidos por los organismos de evaluación de la conformidad que será definido por el Grupo.

Enmienda 42

**Propuesta de Reglamento
Artículo 50 – apartado 6 – letra b**

Texto de la Comisión

b) controlarán y supervisarán las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento, en particular en relación con la notificación de los organismos de evaluación de la conformidad y las tareas conexas establecidas en el artículo 52 del presente Reglamento;

Enmienda

b) controlarán, supervisarán y, **al menos cada dos años, evaluarán** las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento, en particular en relación con la notificación de los organismos de evaluación de la conformidad y las tareas conexas establecidas en el artículo 52 del presente Reglamento;

Justificación

Las disposiciones de control y vigilancia de las autoridades nacionales de supervisión de la certificación han de reforzarse notablemente de cara a evitar la práctica del «shopping» (compra) de la certificación de la UE. Las autoridades nacionales de supervisión de la certificación han de llevar a cabo evaluaciones sobre las actividades de los organismos de evaluación de la conformidad cada dos años.

Enmienda 43**Propuesta de Reglamento****Artículo 50 – apartado 6 – letra b bis (nueva)***Texto de la Comisión**Enmienda*

b bis) notificarán los resultados de las verificaciones contempladas en la letra a) y las evaluaciones contempladas en la letra b) al Grupo Europeo de Certificación de la Ciberseguridad y a ENISA;

Enmienda 44**Propuesta de Reglamento****Artículo 50 – apartado 6 – letra d***Texto de la Comisión**Enmienda*

d) cooperarán con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes europeos de ciberseguridad específicos;

d) cooperarán con otras autoridades nacionales de supervisión de la certificación, ***organismos nacionales de acreditación*** u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes europeos de ciberseguridad específicos;

Justificación

La cooperación entre las autoridades nacionales de supervisión de la certificación y los organismos nacionales de acreditación es muy importante; por ejemplo, estos últimos mantendrán informadas a las primeras sobre la lista de organismos de evaluación de la conformidad, incluida, cuando proceda, cualquier suspensión o retirada de la acreditación a organismos de evaluación de la conformidad.

Enmienda 45

Propuesta de Reglamento

Artículo 50 – apartado 7 – letra e

Texto de la Comisión

e) retirar, con arreglo al Derecho nacional, los certificados que no se ajusten al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad;

Enmienda

e) retirar, con arreglo al Derecho nacional, los certificados que no se ajusten al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad ***e informar al organismo nacional de acreditación en consecuencia;***

Or. en

Justificación

Véase la justificación al artículo 50, apartado 6, letra d).

Enmienda 46

Propuesta de Reglamento

Artículo 50 – apartado 8 – párrafo 1 bis (nuevo)

Texto de la Comisión

Enmienda

La Comisión facilitará un sistema general de apoyo a la información electrónica para realizar dicho intercambio.

Or. en

Justificación

La experiencia demuestra que el intercambio de información entre los Estados miembros se ve a menudo obstaculizado por la falta de un sistema adecuado para realizar tal intercambio.

Enmienda 47

Propuesta de Reglamento

Artículo 53 – apartado 3 – letra –a (nueva)

Texto de la Comisión

Enmienda

–a) proporcionar orientación estratégica y establecer un programa de trabajo sobre las acciones comunes que deben llevarse a cabo a nivel de la Unión para garantizar la aplicación coherente del presente título;

Or. en

Enmienda 48

Propuesta de Reglamento

Artículo 53 – apartado 3 – letra –a bis (nueva)

Texto de la Comisión

Enmienda

–a bis) establecer y actualizar periódicamente una lista de prioridades de los productos y servicios de TIC para los que considera que se precisa un régimen europeo de certificación de la ciberseguridad;

Or. en

Enmienda 49

Propuesta de Reglamento

Artículo 53 – apartado 3 – letra d bis (nueva)

Texto de la Comisión

Enmienda

d bis) adoptar normas vinculantes que establezcan la frecuencia con que las autoridades nacionales de supervisión de la certificación deben llevar a cabo verificaciones de los certificados con

arreglo a la letra a) del apartado 6 del artículo 50, y los criterios, la escala y el alcance de dichas verificaciones, y adoptar criterios comunes acerca del formato de la notificación prevista en la letra b bis) del apartado 6 del artículo 50;

Or. en

Justificación

Vinculada al concepto desarrollado en el artículo 50, apartado 6, letra a).

Enmienda 50

Propuesta de Reglamento
Artículo 53 – apartado 3 – letra e

Texto de la Comisión

e) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar buenas prácticas sobre los regímenes de certificación de la ciberseguridad;

Enmienda

e) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar **información** y buenas prácticas sobre los regímenes de certificación de la ciberseguridad;

Or. en

Enmienda 51

Propuesta de Reglamento
Artículo 53 – apartado 3 – letra f bis (nueva)

Texto de la Comisión

Enmienda

f bis) intercambiar las mejores prácticas en relación con investigaciones de organismos de evaluación de la conformidad y titulares del certificado europeo de ciberseguridad.

Or. en

