**Parlamento Europeo**
2014-2019

*Comisión de Mercado Interior y Protección del Consumidor*

**2017/0225(COD)**

2.3.2018

# ENMIENDAS
# 52 - 366

**Proyecto de opinión**
**Nicola Danti**
(PE616.831v01-00)

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»)

Propuesta de Reglamento
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

AM_Com_LegOpinion

**Enmienda 52**
**Jan Philipp Albrecht**

**Propuesta de Reglamento**
**Título**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Propuesta de | Propuesta de |
| REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO | 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***») | relativo a ENISA, la «Agencia de ***Seguridad de las Redes y de la Información de la Unión Europea***», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ***seguridad informática*** de las tecnologías de la información y la comunicación («Reglamento de ***seguridad informática***») |
| (Texto pertinente a efectos del EEE) | (Texto pertinente a efectos del EEE) |
| | *(Esta enmienda se aplica a la totalidad del texto; su aprobación impone adaptaciones técnicas en todo el texto.)* |

Or. en

*Justificación*

*El prefijo «ciber», derivado de obras de ciencia ficción de la década de 1960, se ha venido empleando cada vez más para describir los aspectos negativos de internet (ciberataque, ciberdelito, etc.), pero es jurídicamente muy ambiguo. Propuesta para sustituir el término «ciberseguridad» por «seguridad informática» para mejorar la seguridad jurídica.*

**Enmienda 53**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Considerando 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (1) Las redes y los sistemas de información y las redes y servicios de telecomunicaciones desempeñan un papel vital para la sociedad y se han convertido en la espina dorsal del crecimiento económico. Las tecnologías de la información y la comunicación ***están en la base de los*** complejos sistemas que sustentan las actividades de la sociedad, garantizan el funcionamiento de nuestras economías en sectores clave como la salud, la energía, las finanzas y el transporte y, en particular, respaldan el funcionamiento del mercado interior. | (1) Las redes y los sistemas de información y las redes y servicios de telecomunicaciones desempeñan un papel vital para la sociedad y se han convertido en la espina dorsal del crecimiento económico. Las tecnologías de la información y la comunicación ***(en lo sucesivo, TIC) constituyen*** complejos sistemas que sustentan las actividades ***cotidianas*** de la sociedad, garantizan el funcionamiento de nuestras economías en sectores clave como la salud, la energía, las finanzas y el transporte y, en particular, respaldan el funcionamiento del mercado interior. |

Or. cs

**Enmienda 54**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (2) La utilización de las redes y los sistemas de información por los ciudadanos, empresas y administraciones de toda la Unión está ya muy generalizada. La digitalización y la conectividad se convierten en elementos básicos en un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera el despliegue en la UE de millones, si no miles de millones, de dispositivos digitales conectados durante la próxima década. Mientras aumenta el número de dispositivos conectados a internet, la seguridad y la resiliencia no se tienen suficientemente en cuenta desde el diseño, lo que provoca insuficiencias en la ciberseguridad. En este contexto, el uso limitado de la certificación priva a los | (2) La utilización de las redes y los sistemas de información por los ciudadanos, empresas y administraciones de toda la Unión está ya muy generalizada. La digitalización y la conectividad se convierten en elementos básicos en un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera el despliegue en la UE de millones, si no miles de millones, de dispositivos digitales conectados durante la próxima década. Mientras aumenta el número de dispositivos conectados a internet, la seguridad y la resiliencia no se tienen suficientemente en cuenta desde el diseño, lo que provoca insuficiencias en la ciberseguridad. En este contexto, el uso limitado de la certificación priva a los |

| | |
|---|---|
| usuarios individuales y las organizaciones de información suficiente sobre las características de ciberseguridad de los productos y servicios de TIC y socava la confianza en las soluciones digitales. | usuarios individuales y las organizaciones de información suficiente sobre las características de ciberseguridad de los productos y servicios de TIC y socava la confianza en las soluciones digitales***, que es esencial para el establecimiento de un mercado único digital***. |

Or. fr

**Enmienda 55**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Considerando 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar ***este riesgo*** para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ciberseguridad en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas. | (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. ***El poder transformador de la inteligencia artificial y el aprendizaje automático será aprovechado por la sociedad en general, pero también por los ciberdelincuentes.*** A fin de atenuar ***estos riesgos*** para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ciberseguridad en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas. |

Or. en

**Enmienda 56**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar este riesgo para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ***ciberseguridad*** en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas. | (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar este riesgo para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ***seguridad frente a los ciberataques*** en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas. |

Or. ro

**Enmienda 57**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los | (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento ***importante*** de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas |

niños. A fin de atenuar este riesgo para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ciberseguridad en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas.

vulnerables como los niños. A fin de atenuar este riesgo para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ciberseguridad en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas.

Or. fr

**Enmienda 58**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (4) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y ciberataques, requieren unas defensas más sólidas. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las respuestas políticas de las autoridades de ciberseguridad y las competencias policiales son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la UE. Esta situación requiere una respuesta y una gestión de crisis efectivas a nivel de la UE, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad europea y la asistencia mutua. En consecuencia, también una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables, y una previsión sistemática de los futuros avances, retos y amenazas, tanto en la Unión como en el mundo, son | (4) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y ciberataques, requieren unas defensas más sólidas ***y seguras***. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las respuestas políticas de las autoridades de ciberseguridad y las competencias policiales son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la UE. Esta situación requiere una respuesta y una gestión de crisis efectivas a nivel de la UE, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad europea y la asistencia mutua. En consecuencia, también una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables, y una previsión sistemática de los futuros avances, retos y amenazas, tanto en la Unión como en el mundo, son |

importantes para los responsables políticos, la industria y los usuarios.

importantes para los responsables políticos, la industria y los usuarios.

Or. ro

**Enmienda 59**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 5**

| *Texto de la Comisión* | *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, 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 | (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 |

nacionales.

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, así como las tecnologías para prevenir ciberataques satisfactorios, 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 60**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Considerando 5**

| *Texto de la Comisión* | *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 | (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.

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 se base en normas europeas o internacionales y*** que aporte requisitos y criterios de evaluación de la ciberseguridad comunes en todos los mercados y sectores nacionales.

Or. en

**Enmienda 61**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 5**

| *Texto de la Comisión* | *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 | (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. | 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 ***de forma homogénea y*** que aporte requisitos y criterios de evaluación de la ciberseguridad comunes en todos los mercados y sectores nacionales. |
| | Or. fr |

**Enmienda 62**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 5 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(5 bis) La seguridad contra los ciberataques es una dimensión de la seguridad en su conjunto, pero la competencia y conocimientos con respecto a la evaluación de la seguridad pertenecen a los Estados miembros. En efecto, la gestión del espacio de libertad, seguridad y justicia es una competencia compartida entre la Unión y los Estados miembros (artículo 4 del TFUE), pero teniendo en cuenta el impacto de la ciberseguridad en la seguridad nacional, es una cuestión de soberanía nacional en muchos aspectos. Por este motivo, en lo que respecta al marco europeo único de certificación, el papel de los Estados miembros y tácito de los organismos nacionales de certificación no debe reducirse a consultivo. Dados sus conocimientos en este sentido, los Estados*** |

***miembros deben desempeñar un papel importante en la nueva arquitectura de certificación de la ciberseguridad.***

Or. ro

**Enmienda 63**
**Antanas Guoga**

**Propuesta de Reglamento**
**Considerando 5 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(5 bis) Mientras que la certificación y otras formas de evaluación de la conformidad de productos y servicios de TIC y procesos desempeña un papel importante, mejorar la ciberseguridad requiere un enfoque multifacético que abarque a las personas, los procesos y las tecnologías. La Unión debe también continuar promoviendo y resaltando rotundamente otros esfuerzos, incluida la educación, la formación y el desarrollo de competencias en materia de ciberseguridad; sensibilizando a nivel corporativo, ejecutivo y de la junta directiva; fomentando el intercambio voluntario de información sobre amenazas cibernéticas; y pasando de un enfoque de la Unión reactivo a uno proactivo, para responder a las amenazas haciendo hincapié en la prevención de los ataques cibernéticos satisfactorios.*** |

Or. en

**Enmienda 64**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 11**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (11) En vista de los crecientes retos en materia de ciberseguridad a que se enfrenta la Unión, deben incrementarse los recursos financieros y humanos asignados a la Agencia, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crítica en el ecosistema de organizaciones que defienden el ecosistema digital europeo. | (11) En vista de los crecientes retos ***y amenazas*** en materia de ciberseguridad a que se enfrenta la Unión, deben incrementarse los recursos financieros y humanos asignados a la Agencia, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crítica en el ecosistema de organizaciones que defienden el ecosistema digital europeo. |

Or. fr

**Enmienda 65**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 21 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(21 bis) Invita a la Comisión a introducir las disposiciones de cooperación obligatorias entre los Estados miembros para asegurar la protección de las infraestructuras críticas.*** |

Or. ro

**Enmienda 66**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 28**

| *Texto de la Comisión* | *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 | (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. | contribuir asimismo a promover las mejores prácticas y soluciones ***de ciberhigiene*** 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 ***multifactor, parches, cifrado, principios de gestión del acceso*** 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. ***La Agencia debe alentar a todos los usuarios finales a adoptar las medidas adecuadas para prevenir y minimizar el impacto de los incidentes que afectan a la seguridad de sus redes y sistemas de información.*** |

Or. en

**Enmienda 67**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 28**

| *Texto de la Comisión* | *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. | (28) La Agencia debe contribuir a la sensibilización del público sobre los riesgos para la ***seguridad informática*** 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 ***y publicación*** de informes ***y guías*** 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 en materia de autenticación***, cifrado, anonimización*** 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 ***y para popularizar a nivel de la Unión la seguridad desde el diseño, la intimidad a través del diseño y los incidentes y sus soluciones***. |
| | Or. en |

*Justificación*

*Detallar los objetivos en línea con el contenido de los artículos.*

**Enmienda 68**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Considerando 28**

| *Texto de la Comisión* | *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. | (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 medidas que pueden adoptarse para protegerse contra*** 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 ***y el uso seguro de los servicios***. |

Or. en

**Enmienda 69**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson, Arndt Kohn**

**Propuesta de Reglamento**
**Considerando 28**

| *Texto de la Comisión* | *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. | (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), ***los ataques de ransomware, el secuestro (hijacking),*** 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. |

Or. en

**Enmienda 70**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson, Arndt Kohn**

**Propuesta de Reglamento**
**Considerando 28 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(28 bis) La Agencia debe promover la integración del principio de seguridad a través del diseño, que es fundamental para mejorar la seguridad de los dispositivos conectados. La seguridad a través del diseño es particularmente importante para los dispositivos dirigidos a usuarios finales vulnerables, como los niños.*** |

Or. en

**Enmienda 71**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 30**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (30) Para asegurar que cumple plenamente sus objetivos, la Agencia debe permanecer en contacto con las instituciones, órganos y organismos pertinentes, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Agencia Europea de Defensa (AED), la Agencia europea para la gestión operativa de los sistemas informáticos de gran magnitud (eu-LISA), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la UE relacionado con la ***ciberseguridad***. También debe mantener contactos con las autoridades encargadas de la protección de datos a fin de intercambiar conocimientos y mejores prácticas y facilitar asesoramiento sobre los aspectos de la | (30) Para asegurar que cumple plenamente sus objetivos, la Agencia debe permanecer en contacto con las instituciones, órganos y organismos pertinentes, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Agencia Europea de Defensa (AED), la Agencia europea para la gestión operativa de los sistemas informáticos de gran magnitud (eu-LISA), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la UE relacionado con la ***seguridad informática***. También debe mantener contactos con las autoridades encargadas de la protección de datos a fin de intercambiar conocimientos y mejores prácticas y facilitar asesoramiento sobre los aspectos de la |

| | |
|---|---|
| ***ciberseguridad*** que podrían repercutir en su trabajo. Los representantes de las autoridades nacionales y de la Unión encargadas de hacer cumplir la ley y proteger los datos deben poder estar representados en el Grupo Permanente de Partes Interesadas de la Agencia. En sus relaciones con los organismos encargados de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en el trabajo de dichos organismos, la Agencia debe respetar los canales de información y las redes existentes. | ***seguridad informática*** que podrían repercutir en su trabajo. Los representantes de las autoridades nacionales y de la Unión encargadas de hacer cumplir la ley y proteger los datos deben poder estar representados en el Grupo Permanente de Partes Interesadas de la Agencia. En sus relaciones con los organismos encargados de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en el trabajo de dichos organismos, la Agencia debe respetar los canales de información y las redes existentes. ***Deben establecerse asociaciones con instituciones académicas que tengan iniciativas de investigación en los ámbitos pertinentes, mientras que la aportación de las organizaciones de consumidores y otras organizaciones debe contar con canales apropiados y analizarse siempre.*** |

Or. en

*Justificación*

*Introducción de la idea de que ENISA debería beneficiarse del conjunto de conocimientos disponibles*

**Enmienda 72**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 33**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (33) La Agencia debe ***desarrollar y mantener sus conocimientos técnicos en materia de certificación de la ciberseguridad con vistas a respaldar la política de la Unión en este ámbito. Debe igualmente*** promover ***la asimilación*** de la certificación ***de la ciberseguridad*** en la Unión***, en particular contribuyendo*** a la | (33) La Agencia debe promover ***el uso*** de la certificación***, evitando al mismo tiempo la fragmentación ocasionada por la falta de coordinación entre los regímenes de certificación existentes*** en la Unión***. La Agencia debe contribuir*** a la creación y mantenimiento de un marco de certificación de la ciberseguridad a nivel de |

creación y mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión, 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.

la Unión ***de conformidad con los artículos 43 a 54 (título III)***, 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 ***único*** digital.

Or. en

**Enmienda 73**
**Liisa Jaakonsaari, Lucy Anderson**

**Propuesta de Reglamento**
**Considerando 35**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ciberseguridad personal. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ciberseguridad. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ciberseguridad de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ciberseguridad, de sus productos y servicios. | (35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ciberseguridad personal. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ciberseguridad. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ciberseguridad de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ciberseguridad, de sus productos y servicios. ***Debe hacerse público en un portal específico cualquier proveedor o fabricante que reciba una advertencia sobre el nivel de ciberseguridad de sus productos.*** |

Or. en

**Enmienda 74**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 35**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ***ciberseguridad*** personal. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ***ciberseguridad***. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ***ciberseguridad*** de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ***ciberseguridad***, de sus productos y servicios. | (35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ***seguridad informática*** personal ***y abstenerse de permitir las ventas o el uso de dispositivos que no cumplan las condiciones mínimas de seguridad***. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ***seguridad informática***. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ***seguridad informática*** de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ***seguridad informática***, de sus productos y servicios. |

Or. en

*Justificación*

*En línea con la introducción de un requisito de seguridad informática de referencia*

**Enmienda 75**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 41**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (41) Para que la Agencia funcione correcta y eficazmente, la Comisión y los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales adecuadas y de experiencia en las áreas funcionales. La Comisión y los Estados miembros deben asimismo tratar de limitar la rotación de sus respectivos representantes en el Consejo de Administración, con el fin de garantizar la continuidad en su labor. | (41) Para que la Agencia funcione correcta y eficazmente, la Comisión y los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales adecuadas y de experiencia en las áreas funcionales. La Comisión y los Estados miembros deben asimismo tratar de limitar la rotación de sus respectivos representantes en el Consejo de Administración, con el fin de garantizar la continuidad en su labor. ***Debido al alto valor de mercado de las competencias requeridas para el trabajo de la Agencia, es necesario garantizar que los salarios y las condiciones sociales ofrecidas a todo el personal de la Agencia sean competitivos y que los mejores profesionales puedan optar por trabajar en ella.*** |

Or. en

*Justificación*

*Enmienda con objeto de contar con el nivel apropiado de experiencia que ENISA necesita para ser un empleador competitivo en un mercado altamente competitivo*

**Enmienda 76**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Considerando 41**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (41) Para que la Agencia funcione correcta y eficazmente, ***la Comisión y*** los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales | (41) Para que la Agencia funcione correcta y eficazmente, los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales |

adecuadas y de experiencia en las áreas funcionales. ***La Comisión y los Estados miembros deben asimismo tratar de limitar la rotación de sus respectivos representantes en el Consejo de Administración, con el fin de garantizar la continuidad en su labor.***

adecuadas y de experiencia en las áreas funcionales.

Or. fr

**Enmienda 77**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 42**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ***ciberseguridad***. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia, previa consulta con la Comisión, y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe tener la posibilidad de crear grupos de trabajo ad hoc para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo ad hoc sean seleccionados entre los expertos de mayor nivel, teniendo | (42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ***seguridad informática***. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia, previa consulta con la Comisión, y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe tener la posibilidad de crear grupos de trabajo ad hoc para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo ad hoc sean seleccionados entre los expertos de mayor nivel, teniendo |

| | |
|---|---|
| debidamente en cuenta la necesidad de lograr un equilibrio representativo, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información. | debidamente en cuenta la necesidad de lograr un equilibrio representativo ***y de género***, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información. |

Or. en

*Justificación*

*Introducción de las modificaciones que añaden el equilibrio de género en algunos de los estratos de ENISA.*

**Enmienda 78**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Considerando 42**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ciberseguridad. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia***, previa consulta con la Comisión,*** y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe | (42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ciberseguridad. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe tener la posibilidad de crear |

| | |
|---|---|
| tener la posibilidad de crear grupos de trabajo ad hoc para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo ad hoc sean seleccionados entre los expertos de mayor nivel, teniendo debidamente en cuenta la necesidad de lograr un equilibrio representativo, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información. | grupos de trabajo ad hoc para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo ad hoc sean seleccionados entre los expertos de mayor nivel, teniendo debidamente en cuenta la necesidad de lograr un equilibrio representativo, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información. |

Or. fr

**Enmienda 79**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 44**

| *Texto de la Comisión* | *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. 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 | (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***, el mundo académico*** 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***, aportando información sobre los productos y servicios de TIC que deben incluirse en los futuros regímenes europeos de certificación de la seguridad informática***. La composición del Grupo Permanente de |

| | |
|---|---|
| interesadas en los trabajos de la Agencia. | 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 ***eficiente y equitativa*** de las partes interesadas en los trabajos de la Agencia. |

Or. en

**Enmienda 80**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Considerando 44**

| *Texto de la Comisión* | *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. 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. | *(No afecta a la versión española.)* |

Or. cs

**Enmienda 81**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Considerando 46**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (46) Con el fin de garantizar la plena autonomía e independencia de la Agencia y para que pueda desempeñar funciones adicionales y nuevas, incluidas tareas de emergencia imprevistas, se considera necesario concederle un presupuesto suficiente y autónomo cuyos ingresos procedan principalmente de una contribución de la Unión y de contribuciones de los terceros países que participen en los trabajos de la Agencia. La mayor parte del personal de la Agencia debe estar dedicado directamente a la aplicación operativa de su mandato. Debe permitirse que el Estado miembro que la acoge, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de la Agencia. El procedimiento presupuestario de la Unión debe seguir siendo aplicable por lo que respecta a las subvenciones imputables al presupuesto general de la Unión. Además, el Tribunal de Cuentas Europeo debe realizar una auditoría de las cuentas de la Agencia para garantizar la transparencia ***y*** la responsabilidad. | (46) Con el fin de garantizar la plena autonomía e independencia de la Agencia y para que pueda desempeñar funciones adicionales y nuevas, incluidas tareas de emergencia imprevistas, se considera necesario concederle un presupuesto suficiente y autónomo cuyos ingresos procedan principalmente de una contribución de la Unión y de contribuciones de los terceros países que participen en los trabajos de la Agencia. La mayor parte del personal de la Agencia debe estar dedicado directamente a la aplicación operativa de su mandato. Debe permitirse que el Estado miembro que la acoge, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de la Agencia. El procedimiento presupuestario de la Unión debe seguir siendo aplicable por lo que respecta a las subvenciones imputables al presupuesto general de la Unión. Además, el Tribunal de Cuentas Europeo debe realizar una auditoría de las cuentas de la Agencia para garantizar la transparencia***,*** la responsabilidad***, la eficiencia y la utilidad de los recursos asignados***. |

Or. cs

**Enmienda 82**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 47**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos | (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos |

del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ***ciberseguridad*** de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ***ciberseguridad*** establecidos en otro lugar, por ejemplo en las normas técnicas.

del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ***seguridad informática*** de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. ***Si bien la certificación para niveles de garantía inferiores a los elevados puede requerir meramente una evaluación de la conformidad, para un nivel de garantía elevado es necesaria una evaluación de seguridad en profundidad, así como una certificación neutral. Por consiguiente, los certificados correspondientes a este nivel de garantía solo deben ser expedidos por las autoridades de supervisión de la ciberseguridad. La expedición de estos certificados debe estar sujeta a revisiones mutuas por pares por parte de otras autoridades de supervisión de la ciberseguridad.*** La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ***seguridad informática*** establecidos en otro lugar, por ejemplo en las normas técnicas.

Or. en

**Enmienda 83**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 47**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (47) La evaluación de la conformidad es el proceso por el que se demuestra que se | (47) La evaluación de la conformidad es el proceso por el que se demuestra que se |

han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente***, distinto del fabricante del producto o del prestador de servicios***. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios ***de hardware y software*** de TIC») por un tercero independiente ***o mediante un procedimiento estricto de autodeclaración de la conformidad según lo indicado en el artículo 2, apartado 16 bis, artículo 46, artículo 50 y artículo 51 del presente Reglamento***. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios ***de hardware y software*** de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

Or. en

**Enmienda 84**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Considerando 47**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad ***de*** un producto, proceso, servicio, sistema, o | (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características ***y prácticas*** de ciberseguridad ***comprendidas en*** un |

| | |
|---|---|
| combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas. | producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC***, así como los procesos y sistemas subyacentes,*** han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas. |

Or. en

**Enmienda 85**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Considerando 47**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido | (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados ***y se debe informar de ello al usuario final***. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los |

| | |
|---|---|
| sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas. | productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas. |
| | Or. en |

**Enmienda 86**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 48**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (48) La certificación de la ciberseguridad desempeña un ***importante*** papel a la hora de aumentar la confianza y la seguridad en los productos y servicios de TIC. El mercado único digital, y en particular la economía de los datos y la internet de las cosas, solo pueden prosperar si el público en general confía en que dichos productos y servicios ofrecen un ***determinado*** nivel de garantía de ciberseguridad. Los vehículos conectados y automatizados, los dispositivos médicos electrónicos, los sistemas de control de la automatización industrial o las redes inteligentes son solo algunos ejemplos de sectores en los que la certificación se utiliza ya ampliamente o es probable que se utilice en un futuro próximo. También en los sectores regulados por la Directiva SRI resulta crítica la certificación de la ciberseguridad. | (48) La certificación ***europea*** de la ciberseguridad desempeña un papel ***esencial*** a la hora de aumentar la confianza y la seguridad en los productos y servicios de TIC. El mercado único digital, y en particular la economía de los datos y la internet de las cosas, solo pueden prosperar si el público en general confía en que dichos productos y servicios ofrecen un ***alto*** nivel de garantía de ciberseguridad. Los vehículos conectados y automatizados, los dispositivos médicos electrónicos, los sistemas de control de la automatización industrial o las redes inteligentes son solo algunos ejemplos de sectores en los que la certificación se utiliza ya ampliamente o es probable que se utilice en un futuro próximo. También en los sectores regulados por la Directiva SRI resulta crítica la certificación de la ciberseguridad. |
| | Or. fr |

**Enmienda 87**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 49**

| *Texto de la Comisión* | *Enmienda* |
| --- | --- |
| (49) En la Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora», la Comisión indicó la necesidad de productos y soluciones de ciberseguridad de alta calidad, asequibles e interoperables. El suministro de los productos y servicios de TIC dentro del mercado único sigue estando muy fragmentado desde el punto de vista geográfico. Esto se debe a que la industria de la ciberseguridad en Europa se ha desarrollado en gran medida a partir de la demanda de los gobiernos nacionales. Además, la falta de soluciones interoperables (normas técnicas), prácticas y mecanismos de certificación a escala de la UE es otra de las carencias que padece el mercado único de la ciberseguridad. Por una parte, esto hace difícil que las empresas europeas compitan a nivel nacional, europeo y mundial; por otra, reduce las opciones de contar con tecnologías de ciberseguridad viables y utilizables a las que puedan acceder particulares y empresas. Del mismo modo, en la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, la Comisión destacó la necesidad de seguridad en los productos y sistemas conectados, indicando que la creación de un marco europeo de seguridad de las TIC que establezca pautas para organizar la certificación de seguridad de las TIC en la Unión podría tanto preservar la confianza en internet como combatir la actual fragmentación del mercado de la ciberseguridad. | (49) En la Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora», la Comisión indicó la necesidad de productos y soluciones de ciberseguridad de alta calidad, asequibles e interoperables. El suministro de los productos y servicios ***de hardware y software*** de TIC dentro del mercado único sigue estando muy fragmentado desde el punto de vista geográfico. Esto se debe a que la industria de la ciberseguridad en Europa se ha desarrollado en gran medida a partir de la demanda de los gobiernos nacionales. Además, la falta de soluciones interoperables (normas técnicas), prácticas y mecanismos de certificación a escala de la UE es otra de las carencias que padece el mercado único de la ciberseguridad. Por una parte, esto hace difícil que las empresas europeas compitan a nivel nacional, europeo y mundial; por otra, reduce las opciones de contar con tecnologías de ciberseguridad viables y utilizables a las que puedan acceder particulares y empresas. Del mismo modo, en la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, la Comisión destacó la necesidad de seguridad en los productos y sistemas conectados, indicando que la creación de un marco europeo de seguridad de las TIC que establezca pautas para organizar la certificación de seguridad de las TIC en la Unión podría tanto preservar la confianza en internet como combatir la actual fragmentación del mercado de la ciberseguridad. |
| | Or. en |

**Enmienda 88**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 50**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (50) En la actualidad, la certificación de la ciberseguridad de los productos y servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real. | (50) En la actualidad, la certificación de la ciberseguridad de los productos y servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales***, con los correspondientes costes adicionales que suponen estos procedimientos***. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real. |

Or. ro

**Enmienda 89**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 50**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (50) En la actualidad, la certificación de la ciberseguridad de los productos y | (50) En la actualidad, la certificación de la ciberseguridad de los productos y |

servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real.

servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía ***basada en los riesgos***, criterios sustantivos y utilización real.

Or. en

**Enmienda 90**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 52**

| *Texto de la Comisión* | *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. El marco europeo debe tener un doble objetivo: por una parte, | (52) Por todo ello, es necesario establecer un marco europeo de certificación de la ***seguridad informática*** que establezca los principales requisitos horizontales para desarrollar regímenes europeos de certificación de la ***seguridad informática*** 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 |

| | |
|---|---|
| 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. | 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 ***seguridad informática*** contradictorias o redundantes y, por ende, reducir los costes para las empresas que operan en el mercado único digital. Los regímenes ***deben guiarse por los principios de seguridad desde el diseño, así como los mencionados en el Reglamento 2016/679. Asimismo,*** 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. |

Or. en

*Justificación*

*Introducir los principios rectores para los regímenes de certificación*

**Enmienda 91**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 52**

| *Texto de la Comisión* | *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. 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 | (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 hardware y software*** 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 hardware y software*** de TIC |

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.

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.

Or. en

**Enmienda 92**
**Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 52**

| *Texto de la Comisión* | *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. 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 | (52) Por todo ello, es necesario ***adoptar un enfoque común y*** 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.

objetivos legítimos de la UE al respecto.

Or. fr

**Enmienda 93**
**Philippe Juvin, Andreas Schwab**

**Propuesta de Reglamento**
**Considerando 52 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(52 bis) Este marco europeo de certificación de la ciberseguridad deberá implantarse de forma homogénea en todos los Estados miembros, a fin de evitar la práctica del «shopping» (compra) de certificaciones, debido a las diferencias de costes o en los niveles de exigencia entre Estados miembros.*** |

Or. fr

**Enmienda 94**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 53**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (53) La Comisión debe estar facultada para adoptar regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del Reglamento. No obstante, | (53) La Comisión debe estar facultada para adoptar regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios ***de hardware y software*** de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del |

los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos.

Reglamento. No obstante, los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos.

Or. en

**Enmienda 95**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Considerando 53**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (53) La Comisión ***debe estar facultada para adoptar*** regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del Reglamento. No obstante, los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos. | (53) ***Los Estados miembros notificarán a*** la Comisión ***sus decisiones en cuanto a los*** regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del Reglamento. No obstante, los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos. |

Or. fr

**Enmienda 96**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 55**

| *Texto de la Comisión* | *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. | (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 desde el diseño en todas las fases del ciclo de vida del producto o servicio.***

Or. en

**Enmienda 97**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 55**

| *Texto de la Comisión* | *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 | (55) El objetivo de los regímenes europeos de certificación de la ciberseguridad debe ser garantizar que los productos y servicios ***de hardware y software*** 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 hardware y software*** de TIC. Los productos y servicios ***de hardware y software*** 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 |

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.

regímenes europeos de certificación de la ciberseguridad. ***Esto se hará mediante una lista de verificación que enumere los riesgos que se espera que afronte el producto o servicio de hardware o software de TIC por parte de una categoría determinada de usuarios en un entorno determinado.*** Las modalidades con que se lograrán tales objetivos para determinados productos y servicios ***de hardware y software*** 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.

Or. en

**Enmienda 98**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Considerando 55**

| *Texto de la Comisión* | *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 | (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.

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. ***Cuando el régimen de certificación prevea marcas o etiquetas, deben señalarse las condiciones en las que pueden utilizarse tales marcas o etiquetas. Las marcas y etiquetas deben ser claras y de fácil comprensión para el usuario final.***

Or. en

**Enmienda 99**
**Dennis de Jong**

**Propuesta de Reglamento**
**Considerando 55**

| *Texto de la Comisión* | *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 | (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. | 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. ***En función del régimen de certificación, los requisitos especificados del régimen podrían, en principio, hacer uso de las mejores prácticas existentes cuando proceda.*** |
| | Or. en |

*Justificación*

*En el caso de las TIC, ya existen muchas mejores prácticas y estas son aceptadas por el colectivo de la seguridad, que abarca la mayoría, si no todos, los casos de vulnerabilidad. Por tanto, un nuevo régimen podría basarse en el conjunto de conocimientos ya existente. Si realizar cambios a estas mejores prácticas redunda en el interés superior de la Unión, entonces sería fácilmente justificable.*

**Enmienda 100**

**Lambert van Nistelrooij**

**Propuesta de Reglamento**
**Considerando 55**

| *Texto de la Comisión* | *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. | (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. ***En función del régimen de certificación, los requisitos especificados del régimen podrían, en*** |

***principio, hacer uso de las mejores prácticas existentes cuando proceda.***

Or. en

*Justificación*

*En el caso de las TIC, ya existen muchas mejores prácticas y estas son aceptadas por el colectivo de la seguridad, que abarca la mayoría, si no todos, los casos de vulnerabilidad. Por tanto, un nuevo régimen podría basarse en el conjunto de conocimientos ya presente y existente. Si realizar cambios a estas mejores prácticas redunda en el interés superior de la Unión, entonces sería, sin duda, fácilmente justificable.*

**Enmienda 101**
**Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Kerstin Westphal, Pina Picierno, Marc Tarabella, Christel Schaldemose**

**Propuesta de Reglamento**
**Considerando 55 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(55 bis) A la luz de las tendencias de innovación y de la creciente accesibilidad y el constante aumento del número de dispositivos de la internet de las cosas en todos los sectores de la sociedad, debe prestarse especial atención a la seguridad de todos los productos de la internet de las cosas, hasta del más simple de ellos. Por lo tanto, dado que la certificación es un método clave para aumentar la confianza en el mercado y aumentar la seguridad y la resiliencia, debe hacerse hincapié en los productos y servicios de la internet de las cosas en el nuevo marco de certificación de la ciberseguridad de la Unión, a fin de hacerlos menos vulnerables y más seguros para los consumidores y las empresas.*** |

Or. en

**Enmienda 102**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. 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***. | (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***,*** servicios ***y procesos*** 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.*** |

**Enmienda 103**
**Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella, Christel Schaldemose**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. 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.*** | (56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. ***Deben delegarse en*** la Comisión ***poderes*** para adoptar ***actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea en lo referente al establecimiento de*** regímenes europeos de certificación de la ciberseguridad ***para productos y servicios de TIC. 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. 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. A la hora de adoptar estos actos delegados,*** la Comisión ***debe basarse en los regímenes de*** certificación de la ciberseguridad ***para*** productos y servicios de TIC ***o en propuestas de regímenes relevantes que proponga ENISA.*** |

Or. en

**Enmienda 104**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. 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***. | (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***. En el régimen debe considerarse el ciclo de vida completo del producto, incluidas las normas aplicables a la retirada de los productos o servicios.*** |

Or. en

**Enmienda 105**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. 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. | (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. ***Los regímenes que establecen marcas o etiquetas podrían ser un incentivo para que las empresas logren las mejores prácticas en materia de seguridad.*** |

Or. en

**Enmienda 106**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. 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. | (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. ***Los requisitos de seguridad deben depender del riesgo resultante del producto o servicio de TIC.*** |

Or. en

**Enmienda 107**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. A | (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.

continuación, la Comisión, sobre la base de las propuestas presentadas por ENISA, ***estaría*** facultada para adoptar el régimen europeo de certificación de la ciberseguridad mediante actos de ejecución ***solo tras haber obtenido la aprobación de los Estados miembros***. 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.

Or. fr

**Enmienda 108**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 56**

| *Texto de la Comisión* | *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. Teniendo en cuenta la finalidad general y los objetivos de seguridad | (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. | 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 hardware y software*** 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 ***basada en los riesgos***: ***elemental***, sustancial o elevado. |

Or. en

**Enmienda 109**
**Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Kerstin Westphal, Pina Picierno, Marc Tarabella**

**Propuesta de Reglamento**
**Considerando 56 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(56 bis) Entre los métodos de evaluación y los procedimientos de evaluación relacionados con cada régimen europeo de certificación de la ciberseguridad, debe promoverse a nivel de la Unión la piratería informática ética, cuyo objetivo es localizar las debilidades y vulnerabilidades de los dispositivos y sistemas de información mediante la anticipación de las acciones y competencias previstas de los piratas informáticos maliciosos.*** |

Or. en

**Enmienda 110**
**Maria Grapini**

**Propuesta de Reglamento**
**Considerando 56 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(56 bis) Es necesario analizar el proceso de certificación europea para evitar el incremento de los costes para los productores.*** |

Or. ro

**Enmienda 111**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución***, a excepción de los casos relacionados con la seguridad nacional de los Estados, el procesamiento de información confidencial y los contratos públicos y de seguridad nacional relacionados***. ***Así se aplicará desde la fecha estipulada por la Comisión en el acto de ejecución, el cual debe conceder a los Estados miembros tiempo suficiente para realizar una transición sosegada y sin incidentes al*** |

***nuevo régimen de certificación***. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. ***En consecuencia, el régimen propuesto debe ser suficientemente flexible y permitir una adaptación eficaz al entorno, en continuo y rápido desarrollo, de la tecnología, debe garantizar la compatibilidad con las normas internacionales y no debe generar obstáculos a la innovación, de modo que solo ofrezca ventajas a los Estados miembros y ninguna dificultad.***

Or. cs

**Enmienda 112**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. ***Tras esta fase inicial, y en función de la madurez de aplicación en los Estados miembros de la Unión y de la criticidad de un producto o servicio, se reconoce que, en el futuro, es posible que empiecen a evolucionar en un enfoque gradual regímenes potencialmente obligatorios para determinados productos y servicios de TIC.*** No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha |

establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. ***Ahora bien, ello debe entenderse sin perjuicio de los sistemas nacionales que cubren los productos, procesos y servicios de TIC utilizados para satisfacer las necesidades de dominio soberano de los Estados miembros, de los que tienen la responsabilidad exclusiva.***

Or. en

**Enmienda 113**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. Sin embargo, ***los requisitos de seguridad informática de referencia deben ser obligatorios y deben aplicarse en todos los dispositivos y servicios del consumidor para abordar los retos de un mundo cada vez más conectado. Estos requisitos mínimos pueden incluir la autenticación, la seguridad de conexiones y parches para las vulnerabilidades descubiertas.*** Con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la |

Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.

Or. en

*Justificación*

*La adición prevé resolver rápidamente la actual falta de requisitos de seguridad informática de referencia armonizados.*

**Enmienda 114**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario***, salvo que se prevea otra cosa en la legislación nacional o*** de la Unión. ***No obstante,*** con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario***. Cuando en el Derecho*** de la Unión ***surja la necesidad específica de que determinados productos o servicios demuestren el cumplimiento de un conjunto de requisitos armonizados en materia de ciberseguridad, los requisitos y el proceso de evaluación y verificación del cumplimiento deben establecerse en la legislación de la Unión de conformidad con el nuevo enfoque.*** Con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de |

certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.

Or. en

**Enmienda 115**
**Dita Charanzová**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario***, salvo que se prevea otra cosa en la legislación nacional o de*** la Unión. ***No obstante,*** con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario***. Sin embargo, ello no debe impedir que*** la Unión ***o las administraciones de los Estados miembros exijan una certificación europea de ciberseguridad, entre otras cosas, como parte de la autorización para proyectos de infraestructura o contratos públicos.*** Con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. |

Or. en

**Enmienda 116**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**

**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, ***excepto para productos y servicios de TIC con elevados requisitos de seguridad y*** salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. |

Or. en

**Enmienda 117**
**Dennis de Jong**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) ***El recurso a la*** certificación europea de la ciberseguridad debe ***seguir siendo voluntario***, salvo que se prevea otra cosa en la legislación ***nacional o*** de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios | (57) ***La seguridad informática de referencia debe regularse en un marco de*** certificación europea de la ciberseguridad ***que*** debe ***ser obligatorio***, salvo que se prevea otra cosa en la legislación de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la |

de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.

ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.

Or. en

**Enmienda 118**
**Lambert van Nistelrooij**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) ***El recurso a la*** certificación europea de la ciberseguridad debe ***seguir siendo voluntario***, salvo que se prevea otra cosa en la legislación ***nacional o*** de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) ***La seguridad informática de referencia debe regularse en un marco de*** certificación europea de la ciberseguridad ***que*** debe ***ser obligatorio***, salvo que se prevea otra cosa en la legislación de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. |

Or. en

*Justificación*

*Voluntary certification will not tackle the introduction of new unsafe ICT products and services. For instance, the number of connected (consumer and business) IoT-devices will grow with millions in the oncoming years. Competition for these products is price based, less on certifications. When ICT products and services don't comply to baseline ICT security requirements they will be used for botnets, remain vulnerable for hacks and privacy infringements. A voluntary certification framework therefore will not solve this issue. It will only work when implemented probably as an mandatory and EU harmonized framework.*

**Enmienda 119**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 57**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente. | (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios ***de hardware y software*** de TIC cubiertos ya por un régimen europeo existente. |

Or. en

**Enmienda 120**
**Roberta Metsola**

**Propuesta de Reglamento**

**Considerando 58**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período ***máximo de cinco años*** y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. | (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos ***de hardware y software*** de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran***. Estos fabricantes también podrán decidir autodeclarar la conformidad con el sistema europeo de certificación de la ciberseguridad pertinente y estarán sujetos al control de la autoridad nacional de supervisión de la certificación, que, a su vez, informará de los resultados de estas evaluaciones al Grupo Europeo de Certificación de la Ciberseguridad y a ENISA.*** Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período ***determinado en el régimen europeo de certificación de la ciberseguridad pertinente*** y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. |

Or. en

**Enmienda 121**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Considerando 58**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. | (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran***. Los productos y servicios con requisitos de seguridad elevados estarán sujetos a la certificación obligatoria por parte de terceros. Para el resto de productos y servicios de TIC, la certificación por parte de terceros será voluntaria, a menos que se especifique lo contrario en la legislación de la Unión***. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. |

Or. en

**Enmienda 122**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 58**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos ***o*** servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. | (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos***,*** servicios ***o procesos*** al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento. |
| | Or. en |

**Enmienda 123**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Considerando 58 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(58 bis) La Agencia debe presentar a la Comisión unos requisitos de seguridad informática de referencia claros y obligatorios que sean aplicables a todos los dispositivos informáticos*** |

***vendidos en la Unión o exportados desde la Unión (en forma si procede, de actos de ejecución). Dichos requisitos deben elaborarse en un plazo de dos años a partir de la fecha de entrada en vigor del presente Reglamento y revisarse cada dos años a partir de esa fecha, a fin de garantizar mejoras constantes y dinámicas. Estos requisitos de seguridad informática de referencia deben exigir, entre otras cosas, que el dispositivo no contenga ningún vulnerabilidad de seguridad conocida, que sea capaz de aceptar actualizaciones de seguridad fiables, que el vendedor notifique a las autoridades competentes las vulnerabilidades conocidas y repare o sustituya el dispositivo afectado, o bien que el vendedor comunique cuándo vencerá el soporte de seguridad para este dispositivo.***

Or. en

*Justificación*

*Es importante lograr un entorno informático resistente para proteger frente a la ciberdelincuencia y proteger los derechos fundamentales de los usuarios de la informática. Por lo tanto, deben establecerse en el presente Reglamento unos objetivos de alto nivel en materia de seguridad informática en favor de una línea de referencia obligatoria en materia de seguridad informática dentro de la Unión.*

**Enmienda 124**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 58 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***(58 bis) Con el fin de garantizar que la acreditación se lleve a cabo de manera uniforme en toda la Unión, los organismos nacionales de acreditación se someterán a una evaluación por pares coordinada por ENISA.*** |

**Enmienda 125**
**Roberta Metsola**

**Propuesta de Reglamento**
**Considerando 59**

| *Texto de la Comisión* | *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. | (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 hardware y software*** de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes de ciberseguridad específicos. ***Además, deben supervisar y verificar el cumplimiento de las autodeclaraciones de conformidad y que los certificados europeos de ciberseguridad hayan sido expedidos por organismos de evaluación de la conformidad, con los requisitos*** |

***establecidos en el presente Reglamento, incluidas las normas adoptadas por el Grupo Europeo de Certificación de la Ciberseguridad y los requisitos establecidos en el régimen europeo de certificación de la ciberseguridad correspondiente.***

Or. en

**Enmienda 126**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Considerando 65**

| *Texto de la Comisión* | *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. | (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***,*** servicios ***y procesos*** 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. |

Or. en

**Enmienda 127**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Considerando 66**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| (66) Las actividades de la Agencia deben evaluarse de modo independiente. La evaluación debe ***tener en cuenta*** el | (66) Las actividades de la Agencia deben evaluarse de modo independiente. La evaluación debe ***incluir la exactitud y*** |

| | |
|---|---|
| logro de sus objetivos ***por parte de la Agencia,*** sus prácticas de trabajo y la pertinencia de sus tareas. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad. | ***utilidad de los recursos asignados a la Agencia, la eficacia en*** el logro de sus objetivos ***y una descripción de*** sus prácticas de trabajo y la pertinencia de sus tareas. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad. |

Or. cs

**Enmienda 128**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 1 – párrafo 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) establece los objetivos, funciones y aspectos organizativos de ENISA, la «Agencia de ***Ciberseguridad de la UE», denominada en lo sucesivo*** «la Agencia»; y | a) establece los objetivos, funciones y aspectos organizativos de ENISA, la Agencia de ***Seguridad de las Redes y de la Información de la Unión Europea (***«la Agencia»***)***; y |

Or. en

*Justificación*

*Propuesta para mantener el nombre original de ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea).*

**Enmienda 129**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 1 – párrafo 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar | b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar |

| | |
|---|---|
| un nivel adecuado de ciberseguridad de los productos y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión. | un nivel adecuado de ciberseguridad de los productos***, procesos*** y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión.<br>***(Esta enmienda se aplica a la totalidad del texto; su aprobación impone adaptaciones técnicas en todo el texto.)*** |

Or. en

**Enmienda 130**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 1 – párrafo 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión. | b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos***, procesos*** y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión. |

Or. en

*Justificación*

*La ciberseguridad es un objetivo móvil, por lo que la certificación del proceso, como el ciclo de vida completo del producto, debe formar parte del ámbito de aplicación del Reglamento.*

**Enmienda 131**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 1 – párrafo 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos ***y*** servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación ***de carácter voluntario u obligatorio*** contenidas en otros actos de la Unión. | b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos**,** servicios ***y procesos*** de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación contenidas en otros actos de la Unión. |

Or. en

**Enmienda 132**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 1 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis) «ciberhigiene», medidas rutinarias, sencillas y establecidas, como la autenticación multifactor, los parches, el cifrado y la gestión del acceso, que los usuarios finales pueden adoptar para minimizar los riesgos de las amenazas cibernéticas;*** |

Or. en

**Enmienda 133**
**Eva Maydell**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 8 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***8 bis) «higiene cibernética», el establecimiento de medidas rutinarias, que los usuarios y las empresas pueden*** |

***adoptar para minimizar los riesgos de las amenazas cibernéticas y protegerse cuando estén en línea.***

Or. en

**Enmienda 134**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 9**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos ***y*** servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico; | 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas ***de conformidad con el Reglamento (UE) 2012/1025*** y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos***,*** servicios ***y procesos*** de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico; |

Or. en

**Enmienda 135**
**Roberta Metsola, Eva Maydell, Lara Comi, Pascal Arimont, Antonio López-Istúriz White, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 9**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos y servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de | 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos y servicios ***de hardware y software*** de tecnologías de la información y la comunicación (TIC) incluidos en el |

| | |
|---|---|
| dicho régimen específico; | ámbito de aplicación de dicho régimen específico; |

Or. en

**Enmienda 136**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 9**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones***, requisitos técnicos***, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos ***y*** servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico; | 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos y servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico; |

Or. en

**Enmienda 137**
**Eva Maydell**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 10**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; | 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto***, proceso, sistema*** o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; |

Or. en

**Enmienda 138**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 10**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; | 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto***, proceso*** o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; |

Or. en

*Justificación*

*Esta enmienda se aplica a la totalidad del texto; su adopción impone adaptaciones técnicas en todo el texto.*

**Enmienda 139**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 10**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto ***o*** servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; | 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto***,*** servicio ***o proceso*** de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad; |

Or. en

**Enmienda 140**

**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**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 seguridad informática en su territorio;*** |

Or. en

*Justificación*

*El concepto se usó en el texto sin una definición adecuada.*

**Enmienda 141**
**Eva Maydell**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 11 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***11 bis) «proceso y sistema de TIC», un conjunto de procedimientos integrados en el desarrollo, el despliegue y el mantenimiento de productos y servicios de TIC;*** |

Or. en

**Enmienda 142**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 15**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 15) «organismo de evaluación de la conformidad», el organismo de evaluación de la conformidad tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008; | 15) «organismo de evaluación de la conformidad», el organismo de evaluación de la conformidad ***de un Estado miembro que lleva a cabo actividades de evaluación de la conformidad, incluida la calibración, el ensayo, la certificación y la inspección*** tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008; |

Or. en

**Enmienda 143**
**Roberta Metsola, Lara Comi, Antonio López-Istúriz White, Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 16 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***16 bis) «autodeclaración de conformidad», la declaración por parte del fabricante que certifica que su producto o servicio de TIC es conforme con los regímenes europeos de certificación de la ciberseguridad especificados;*** |

Or. en

**Enmienda 144**
**Andreas Schwab**

**Propuesta de Reglamento**
**Artículo 2 – párrafo 1 – punto 16 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***16 bis) «autodeclaración de conformidad», la declaración mediante la cual el fabricante demuestra que se han cumplido los requisitos especificados relacionados con un producto o servicio;*** |

Or. en

**Enmienda 145**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Título II**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ENISA – la «Agencia de ***Ciberseguridad de la UE»*** | ENISA – la Agencia ***de Seguridad de las Redes y de la Información de la Unión Europea*** |

Or. en

*Justificación*

*En línea con la propuesta para mantener el nombre original de ENISA (Agencia Europea de Seguridad de las Redes y de la Información).*

**Enmienda 146**
**Maria Grapini**

**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 a un elevado nivel de ***seguridad de la información a fin de evitar los ciberataques*** dentro de la Unión. |

Or. ro

**Enmienda 147**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**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 ***conseguir*** un elevado nivel de ciberseguridad dentro de la Unión. |

Or. en

*Justificación*

*El cambio consiste en elevar las expectativas, en línea con el ámbito de aplicación de la propuesta.*

**Enmienda 148**
**Maria Grapini**

**Propuesta de Reglamento**
**Artículo 3 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. La Agencia desempeñará los cometidos que le confieran los actos de la Unión que establecen medidas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de ***ciberseguridad***. | 2. La Agencia desempeñará los cometidos que le confieran los actos de la Unión que establecen medidas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de ***seguridad de la información***. |

Or. ro

**Enmienda 149**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 3 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|

***2 bis. La Agencia asistirá a los Estados miembros y a los organismos de la Unión a la hora de establecer políticas y prácticas para la gestión responsable y la divulgación coordinada de las vulnerabilidades de los productos y servicios de TIC que no son de conocimiento público.***

Or. en

*Justificación*

*Las políticas deben ser coherentes con las directrices y las recomendaciones indicadas en las normas internacionales ISO/IEC 29147:2014 e ISO/IEC 30111.*

**Enmienda 150**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 3 – apartado 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3. Los objetivos y cometidos de la Agencia se entenderán sin perjuicio de las competencias de los Estados miembros en materia de ***ciberseguridad y, en todo caso, sin perjuicio de las actividades relacionadas con la seguridad pública, la defensa, la*** seguridad ***nacional y las actividades del Estado en ámbitos del Derecho penal***. | 3. Los objetivos y cometidos de la Agencia se entenderán sin perjuicio de las competencias ***exclusivas*** de los Estados miembros en materia de seguridad ***informática***. |

Or. en

*Justificación*

*No debe haber ampliaciones de las limitaciones resultantes de los tratados.*

**Enmienda 151**
**Maria Grapini**

**Propuesta de Reglamento**
**Artículo 4 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. La Agencia asistirá a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas relativas a la ***ciberseguridad***. | 2. La Agencia asistirá a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas relativas a la ***seguridad de la información, a fin de evitar los ciberataques***. |

Or. ro

**Enmienda 152**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 4 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Agencia fomentará la cooperación y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, incluido el sector privado, sobre las cuestiones relacionadas con la ***ciberseguridad***. | 4. La Agencia fomentará la cooperación y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, incluido el sector privado***, las organizaciones de consumidores y otras organizaciones de la sociedad civil***, sobre las cuestiones relacionadas con la ***seguridad informática***. |

Or. en

*Justificación*

*La referencia al sector privado requería una ampliación adecuada a otras partes interesadas importantes, en particular debido a que el mayor impacto se da en los consumidores*

**Enmienda 153**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 4 – apartado 6**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 6. La Agencia promoverá el uso de la certificación***, 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 mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión de conformidad con ***los artículos 43 a 54 (***título III***)***, 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 ***único*** digital. |

Or. en

**Enmienda 154**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 4 – apartado 7**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad. | 7. La Agencia promoverá un alto nivel de ***ciberhigiene y*** sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad. |

Or. en

**Enmienda 155**
**Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 4 – apartado 7**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad. | 7. La Agencia promoverá un alto nivel de ***información y*** sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad. |

Or. fr

**Enmienda 156**
**Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 4 – apartado 7**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad. | 7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos***, autoridades*** y empresas en torno a las cuestiones relacionadas con la ciberseguridad. |

Or. en

**Enmienda 157**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 4 – apartado 7 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***7 bis. La Agencia asistirá y asesorará a los Estados miembros y a los organismos de la Unión en el establecimiento de políticas y prácticas que promuevan la gestión responsable y la divulgación coordinada de las vulnerabilidades en los productos y servicios de TIC que no sean de conocimiento público, como el establecimiento de procesos gubernamentales de revisión de la*** |

***divulgación de vulnerabilidades y políticas coordinadas de divulgación de vulnerabilidades.***

Or. en

**Enmienda 158**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 4 – apartado 7 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***7 bis. La Agencia asistirá y asesorará a los Estados miembros y a los organismos de la Unión en el establecimiento de políticas y prácticas que promuevan la gestión responsable y la divulgación coordinada de las vulnerabilidades en los productos y servicios de TIC que no sean de conocimiento público, entre otros, en el establecimiento de procesos gubernamentales de revisión de la divulgación de vulnerabilidades y políticas coordinadas de divulgación de vulnerabilidades.*** |

Or. en

*Justificación*

*Esta tarea se ejecutará de conformidad con las directrices y las recomendaciones indicadas en las normas internacionales ISO/IEC 29147:2014 e ISO/IEC 30111.*

**Enmienda 159**
**Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Pina Picierno**

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|

| | |
|---|---|
| 1. Prestando asistencia y asesoramiento***, en particular emitiendo su dictamen independiente y aportando trabajos preparatorios,*** en el desarrollo y la revisión de la política y la legislación de la Unión en el ámbito de la ciberseguridad, así como las iniciativas políticas y legislativas sectoriales cuando estén presentes cuestiones relacionadas con la ciberseguridad. | 1. Prestando asistencia y asesoramiento en el desarrollo y la revisión de la política y la legislación de la Unión en el ámbito de la ciberseguridad, así como las iniciativas políticas y legislativas sectoriales cuando estén presentes cuestiones relacionadas con la ciberseguridad. |

Or. en

*Justificación*

*Se debe ofrecer a la Agencia una libre elección de instrumentos para llevar a cabo sus tareas.*

**Enmienda 160**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y la legislación de la Unión en materia de ciberseguridad, especialmente en relación con la Directiva (UE) 2016/1148, en particular a través de dictámenes, directrices, recomendaciones y mejores prácticas sobre temas como la gestión de riesgos, la notificación de incidentes y la comunicación de información, así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto. | 2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y la legislación de la Unión en materia de ciberseguridad, especialmente en relación con la Directiva (UE) 2016/1148, en particular a través de dictámenes, directrices, recomendaciones y mejores prácticas sobre temas como la gestión de riesgos, la notificación de incidentes y la comunicación de información, ***las medidas técnicas y organizativas, en particular el establecimiento de programas coordinados de divulgación de vulnerabilidades,*** así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto. |

Or. en

*Justificación*

*The NIS-Directive leaves open the range of measures a company can take in order to ensure compliance as part of the "technical and organisational measures" prescribed in Article 14 of Directive (EU) 2016/1148. These measures can include the establishment of a coordinated vulnerability programme, and Member states may explicitly consider parameters regarding the establishment of such a programme in transposing the NIS Directive. ENISA can provide guidelines on how to create such a CVD-programme in order to create a consistent European approach to coordinated vulnerability disclosure that is consistent with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.*

**Enmienda 161**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 bis**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. Asistiendo al Comité Europeo de Protección de Datos establecido por el Reglamento (UE) 2016/679 en el desarrollo de directrices para especificar a nivel técnico las condiciones que permiten el uso lícito de datos personales por parte de los responsables del tratamiento de datos para fines de seguridad informática con el objetivo de proteger su infraestructura mediante la detección y el bloqueo de los ataques contra sus sistemas de información, en el contexto de: i)) Reglamento (UE) 2016/679[1 bis]; ii)) Directiva (UE) 2016/1148[1 ter]; y iii) Directiva 2002/58/CEC[1 quater];*** |
| | ***[1 bis] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).*** |

*[1 ter] (EU) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).*

*[1 quater] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 11*

Or. en

*Justificación*

*Establecer mecanismos de cooperación adecuados.*

**Enmienda 162**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 bis**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. Proponiendo un plan que establezca las funciones, las responsabilidades y los derechos y las obligaciones legales de los investigadores, proveedores, fabricantes, CERT y CSIRT en un programa coordinado de divulgación de vulnerabilidades, en particular en los casos de divulgaciones de vulnerabilidades multipartitas que afecten a múltiples detectores y proveedores de vulnerabilidades en diferentes Estados miembros.*** |

Or. en

*Justificación*

*Las vulnerabilidades Meltdown y Spectre han demostrado la necesidad de programas coordinados de divulgación de vulnerabilidades a escala de la Unión cuyo alcance vaya más allá de los operadores de servicios esenciales. Este plan será coherente con las directrices y las recomendaciones indicadas en las normas ISO/IEC 29147:2014 e ISO/IEC 30111.*

**Enmienda 163**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 ter (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 ter. Proponiendo políticas con el objetivo de garantizar que los fabricantes de TIC actúan con la debida diligencia en relación con la reparación oportuna de vulnerabilidades de seguridad informática en sus productos y servicios a fin de evitar exponer indebidamente a sus usuarios a la ciberdelincuencia.*** |

Or. en

*Justificación*

*Establecer un desglose de responsabilidades correcto es esencial para animar a todas las partes a actuar con la debida diligencia.*

**Enmienda 164**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 quater (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 quater. Proponiendo políticas que establezcan un sólido marco de obligaciones y responsabilidades para todas las partes interesadas que participan*** |

***en los ecosistemas de las TIC.***

Or. en

*Justificación*

*Fomentar que todas las partes interesadas actúen con la debida diligencia.*

**Enmienda 165**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 quinquies (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 quinquies. Proponiendo políticas que refuercen la normativa sobre las responsabilidades de los operadores de infraestructuras de red fundamentales en caso de ataque contra sus sistemas de información que afecte a sus usuarios debido a la falta de diligencia debida por parte de algunos de los usuarios o por el propio operador, cuando el operador no haya tomado todas las medidas razonables para evitar el accidente o atenuar sus efectos sobre todos los usuarios.*** |

Or. en

*Justificación*

*Los operadores de infraestructuras críticas deben encargarse de obtener garantías de que solo los usuarios y participantes seguros y fiables utilizarán su infraestructura y, en caso necesario, de aislar a los que no son seguros para evitar incidentes.*

**Enmienda 166**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 sexies (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 sexies. Proponiendo políticas para limitar la adquisición y uso de vulnerabilidades del tipo «Zero days» por las autoridades públicas para atacar sistemas de información; fomentando auditorías de los programas informáticos y financiando a personal experto.*** |

Or. en

*Justificación*

*Mediante la creación, la adquisición y explotación de «puertas traseras» en los sistemas informáticos con el dinero de los contribuyentes, los organismos públicos están poniendo en riesgo la seguridad de los ciudadanos. Para proteger a otras partes interesadas que tratan de manera responsable esas vulnerabilidades, la Agencia debe proponer políticas en favor del intercambio responsable de información sobre las vulnerabilidades de seguridad del tipo «Zero days» y de otros tipos que todavía no son de conocimiento público, y que faciliten la eliminación de las vulnerabilidades.*

**Enmienda 167**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 septies (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 septies. Proponiendo políticas para que las autoridades públicas, las empresas privadas, los investigadores, las universidades y otras partes interesadas publiquen todas las vulnerabilidades de seguridad esenciales que aún no son conocidas públicamente en el marco de una divulgación responsable.*** |

Or. en

*Justificación*

*Hacen falta políticas adecuadas de la Unión para aplicar procesos coherentes de divulgación*

*responsable en toda la Unión.*

**Enmienda 168**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 2 octies**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 octies. Proponiendo políticas de ampliación de la utilización de «códigos fuente abiertos verificables» para soluciones informáticas en el sector público y para el uso conexo de herramientas automatizadas para facilitar el examen del código fuente y comprobar fácilmente la ausencia de puertas traseras y otras posibles vulnerabilidades en materia de seguridad.*** |

Or. en

*Justificación*

*El uso de programas de código abierto debe fomentarse en las administraciones públicas que también deben aceptar las responsabilidades correspondientes a la comprobación del código fuente de las aplicaciones que utilicen (ante la presencia/ausencia de grandes vulnerabilidades de seguridad informática).*

**Enmienda 169**
**Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Marc Tarabella, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 4 – punto 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2) la promoción de una mejora del nivel de seguridad de las comunicaciones electrónicas, en particular ofreciendo asistencia y asesoramiento y facilitando el intercambio de mejores prácticas entre las | 2) la promoción de una mejora del nivel de seguridad de las comunicaciones electrónicas***, el almacenamiento de datos y el tratamiento de datos***, en particular ofreciendo asistencia y asesoramiento y |

| | |
|---|---|
| autoridades competentes. | facilitando el intercambio de mejores prácticas entre las autoridades competentes. |

Or. en

**Enmienda 170**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 5 – párrafo 1 – apartado 4 – punto 2 bis**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis) el desarrollo y la promoción de políticas que sostengan la disponibilidad general o la integridad del núcleo público de la internet abierta, que proporcionen la funcionalidad esencial a internet en su conjunto y que respalden su funcionamiento normal, incluidas, entre otras cosas, la seguridad y la estabilidad de los protocolos clave (en particular, DNS, BGP e IPv6), el funcionamiento del sistema de nombres de dominio (incluidos los de todos los dominios de nivel superior) y el funcionamiento de la zona raíz*** |

Or. en

*Justificación*

*La protección del núcleo público de internet es una norma emergente que cuenta con el apoyo de la Comisión Mundial sobre la Estabilidad en el Ciberespacio, que recibió su mandato de las conclusiones de la Cuarta Conferencia Global sobre el Ciberespacio (GCCS) celebrada en 2015 en La Haya, así como del Quinto Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas.*

**Enmienda 171**
**Eva Maydell**

**Propuesta de Reglamento**
**Artículo 6 – apartado 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) a los Estados miembros en sus esfuerzos por mejorar la prevención, detección, análisis y capacidad de respuesta a problemas e incidentes de ciberseguridad, proporcionándoles los conocimientos teóricos y prácticos necesarios***;*** | a) a los Estados miembros en sus esfuerzos por mejorar la prevención, detección, análisis y capacidad de respuesta a problemas e incidentes de ciberseguridad, proporcionándoles los conocimientos teóricos y prácticos necesarios***, también con un conjunto de rutinas de higiene cibernética que habrán de seguir los miembros del personal y los ciudadanos.*** |

Or. en

**Enmienda 172**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 6 – apartado 1 – letra a bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***a bis) a los Estados miembros y a los organismos de la Unión en el establecimiento y la aplicación de políticas coordinadas de divulgación de vulnerabilidades y procesos gubernamentales de revisión de la divulgación de vulnerabilidades, cuyas prácticas y determinaciones deben ser transparentes y estar sujetas a supervisión independiente;*** |

Or. en

*Justificación*

*Un proceso gubernamental de revisión de la divulgación de vulnerabilidades implica la gestión de las vulnerabilidades descubiertas por las agencias gubernamentales y establece un proceso que determina cuándo y cómo la agencia gubernamental debe liberar la vulnerabilidad en su poder. Garantizar que los gobiernos y sus agencias cuenten con políticas sólidas para revisar y coordinar la divulgación de las vulnerabilidades es una norma fundamental que debe avanzar en la Unión.*

**Enmienda 173**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 6 – apartado 1 – letra a bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***a bis) a los Estados miembros y a los organismos de la Unión en el establecimiento y la aplicación de políticas coordinadas de divulgación de vulnerabilidades y procesos gubernamentales de igualdad de vulnerabilidades, cuyas prácticas y determinaciones están sujetas a transparencia y supervisión independiente;*** |

Or. en

**Enmienda 174**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 6 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. La Agencia facilitará el establecimiento de centros sectoriales de puesta en común y análisis de la información (ISAC) y les prestará un apoyo continuado, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, aportando mejores prácticas y orientaciones sobre las herramientas disponibles, el procedimiento y la manera de abordar los asuntos normativos relacionados con el intercambio de información. | 2. La Agencia facilitará el establecimiento de centros sectoriales de puesta en común y análisis de la información (ISAC) y les prestará un apoyo continuado, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, aportando mejores prácticas y orientaciones sobre las herramientas disponibles, el procedimiento***, los principios de ciberhigiene*** y la manera de abordar los asuntos normativos relacionados con el intercambio de información. |

Or. en

**Enmienda 175**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 6 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. La Agencia facilitará el establecimiento y la puesta en marcha de un proyecto de seguridad informática europeo a largo plazo para apoyar el desarrollo de una industria de seguridad informática de la Unión independiente, e integrar la seguridad informática en todas las novedades informáticas de la Unión.*** |

Or. en

*Justificación*

*ENISA debe asesorar a los legisladores en relación con la preparación de políticas que permitan a la Unión ponerse a la altura de las industrias de seguridad informática en terceros países. El proyecto debe ser comparable en escala a lo que ya se ha logrado anteriormente en el sector aeronáutico (Airbus, por ejemplo). Esto es necesario para desarrollar una industria de las TIC de la Unión más sólida, soberana y fiable [véase el estudio de la Unidad de Prospectiva Científica (STOA) PE 614.531].*

**Enmienda 176**
**Maria Grapini**

**Propuesta de Reglamento**
**Artículo 7 – apartado 5 – párrafo 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| A petición de ***dos*** o más Estados miembros afectados y con el único objetivo de prestar asesoramiento para la prevención de incidentes futuros, la Agencia prestará apoyo para que se realice, o realizará, una investigación técnica ex post tras las notificaciones por las empresas afectadas de incidentes que tengan un impacto | A petición de ***uno*** o más Estados miembros afectados y con el único objetivo de prestar asesoramiento para la prevención de incidentes futuros, la Agencia prestará apoyo para que se realice, o realizará, una investigación técnica ex post tras las notificaciones por las empresas afectadas de incidentes que tengan un impacto |

| | |
|---|---|
| significativo o sustancial con arreglo a la Directiva (UE) 2016/1148. La Agencia también llevará a cabo dicha investigación tras una solicitud debidamente justificada de la Comisión de acuerdo con los Estados miembros afectados en caso de incidentes que afecten a más de dos Estados miembros. | significativo o sustancial con arreglo a la Directiva (UE) 2016/1148. La Agencia también llevará a cabo dicha investigación tras una solicitud debidamente justificada de la Comisión de acuerdo con los Estados miembros afectados en caso de incidentes que afecten a más de dos Estados miembros. |

Or. ro

**Enmienda 177**
**Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 7 – apartado 8 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) agregación de los informes procedentes de fuentes nacionales, con vistas a contribuir a la creación de una perspectiva común de la situación; | a) agregación de los informes procedentes de fuentes nacionales ***e internacionales***, con vistas a contribuir a la creación de una perspectiva común de la situación; |

Or. en

**Enmienda 178**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 7 - apartado 8 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) instaurar sistemas de certificación para desalentar la aplicación por los fabricantes y proveedores de servicios de TIC de puertas traseras secretas que debilitan deliberadamente la seguridad informática de los productos y servicios comerciales y tienen un impacto negativo en la seguridad general de internet.*** |

Or. en

*Justificación*

*Esta evaluación debe reconocerse como uno de los principales objetivos de los regímenes de certificación*

**Enmienda 179**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 7 – apartado 8 – letra e bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***e bis) asistencia y asesoramiento a los Estados miembros en relación con el establecimiento y la aplicación de políticas coordinadas de divulgación de vulnerabilidades y procesos gubernamentales de revisión de la divulgación de vulnerabilidades.*** |

Or. en

*Justificación*

*Esta tarea se ejecutará de conformidad con las directrices y las recomendaciones indicadas en las normas ISO/IEC 29147:2014 e ISO/IEC 30111.*

**Enmienda 180**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra a – punto 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1) preparar propuestas de regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC de conformidad con el artículo 44 del presente Reglamento; | 1) ***en cooperación con las partes interesadas de la industria en un proceso formal, normalizado y transparente, identificar y*** preparar propuestas de regímenes europeos de certificación de la ciberseguridad para productos y servicios |

de TIC de conformidad con el artículo 44 del presente Reglamento;

Or. en

**Enmienda 181**
**Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Pina Picierno, Marc Tarabella, Christel Schaldemose**

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

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis) llevar a cabo controles ex post periódicos e independientes sobre la conformidad de los productos y servicios de TIC certificados con el presente Reglamento;*** |

Or. en

*Justificación*

*Junto con la supervisión a nivel de los Estados miembros, debe haber una supervisión a nivel de la Unión, a fin de asegurar que la conformidad se garantice de forma coordinada en toda la Unión.*

**Enmienda 182**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra a – punto 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3) recopilar y publicar directrices y desarrollar buenas prácticas relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la industria. | 3) recopilar y publicar directrices y desarrollar buenas prácticas***, incluidos los principios de ciberhigiene,*** relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la |

| | |
|---|---|
| | industria ***en un proceso formal, normalizado y transparente***. |

Or. en

**Enmienda 183**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra a – punto 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3) recopilar y publicar directrices y desarrollar buenas prácticas relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la industria. | 3) recopilar y publicar directrices y desarrollar buenas prácticas relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la industria ***en un proceso formal, normalizado y transparente***. |

Or. en

**Enmienda 184**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra a – punto 3 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***3 bis) en consulta con todas las partes interesadas pertinentes, determinar si las normas o los procesos de certificación todavía no existen a nivel mundial para las necesidades identificadas, y si se determina que existen lagunas, pedir a las organizaciones de desarrollo de normas que elaboren normas o procesos.*** |

Or. en

**Enmienda 185**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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***. | b) ***Consultará a las organizaciones de normalización*** europeas e internacionales ***sobre el desarrollo de normas*** para la gestión de riesgos y para la seguridad de los productos y servicios de TIC ***y facilitará el establecimiento y la adopción de las normas europeas e internacionales pertinentes***. |

Or. en

**Enmienda 186**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 8 – apartado 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 | b) Facilitará el establecimiento y la adopción de normas europeas ***o*** 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. | nacionales de los Estados miembros, con arreglo al artículo 19, apartado 2, de la Directiva (UE) 2016/1148. |

Or. en

**Enmienda 187**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra b bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***b bis) Elaborará, en colaboración con los Estados miembros, directrices y orientaciones relativas a las áreas técnicas mencionadas en la letra b), así como en relación con las normas ya existentes, en particular las normas nacionales de los Estados miembros que permitirían cubrir esas áreas.*** |

Or. en

**Enmienda 188**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 8 – párrafo 1 – letra b bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***b bis) Dará prioridad a sus trabajos sobre el inventario de los regímenes nacionales existentes, así como la elaboración de directrices para una posible armonización de estos regímenes con el fin de crear un reconocimiento mutuo en la Unión.*** |

Or. en

**Enmienda 189**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 8 - párrafo 1 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) Instaurará sistemas de certificación para desalentar la aplicación por los fabricantes y proveedores de servicios de TIC de puertas traseras secretas que debilitan deliberadamente la seguridad informática de los productos y servicios comerciales y tienen un impacto negativo en la seguridad general de internet.*** |

Or. en

*Justificación*

*Esta evaluación debe reconocerse como uno de los principales objetivos de los regímenes de certificación*

**Enmienda 190**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 8 - párrafo 1 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) Apoyará y promoverá el desarrollo y la aplicación de políticas coordinadas de divulgación de vulnerabilidades y procesos gubernamentales de revisión de la divulgación de vulnerabilidades.*** |

Or. en

**Enmienda 191**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra d**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| d) reunirá, organizará y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión; | d) reunirá, organizará y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión***, incluida la información sobre incidentes de ciberseguridad significativos, violaciones de datos importantes, e información sobre los proveedores o fabricantes que hayan recibido una advertencia de ENISA en relación con el nivel de ciberseguridad de sus productos***; |

Or. en

**Enmienda 192**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra d**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| d) reunirá, ***organizará*** y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión; | *(No afecta a la versión española.)* |

Or. cs

**Enmienda 193**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra e**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| e) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas para usuarios individuales, dirigidas a ciudadanos y organizaciones; | e) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas ***de ciberhigiene*** para usuarios individuales, dirigidas a ciudadanos y organizaciones; |

Or. en

**Enmienda 194**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra e**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| e) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas para usuarios ***individuales***, dirigidas a ciudadanos y organizaciones; | e) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas para usuarios, dirigidas a ciudadanos y organizaciones; |

Or. en

**Enmienda 195**
**Eva Maydell**

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra e bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***e bis) apoyará una cooperación más estrecha con los Estados miembros en relación con la educación en materia de ciberseguridad, la sensibilización y la higiene cibernética;*** |

Or. en

**Enmienda 196**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra g bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***g bis) favorecerá la adopción generalizada por parte de todos los agentes del Mercado Único Digital de la Unión de medidas de seguridad informática preventivas sólidas y protección de datos fiable y de tecnologías de mejora de la intimidad fiables como primera línea de defensa contra los ataques contra los sistemas de información.*** |

Or. en

*Justificación*

*Enmienda basada en el dictamen del SEPD (para las tecnologías de mejora de la intimidad). El papel de ENISA debe ir claramente más allá del soporte a los Estados miembros, la Comisión Europea y las agencias de la Unión, pero también debe ser más visible en el sector y entre el público en general.*

**Enmienda 197**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 9 – párrafo 1 – letra g bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***g bis) apoyará una coordinación más estrecha y el intercambio de mejores prácticas entre los Estados miembros sobre educación en materia de ciberseguridad y sensibilización en materia de ciberhigiene, facilitando la creación y el mantenimiento de una red de puntos de contacto de la educación nacional;*** |

Or. en

**Enmienda 198**
**Inese Vaidere**

**Propuesta de Reglamento**
**Artículo 10 – párrafo 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo; | a) ***garantizará la consulta previa con los grupos de usuarios pertinentes y*** asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo; |

Or. en

**Enmienda 199**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 10 – párrafo 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en ***el ámbito*** de la ciberseguridad, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo; | a) asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en ***los ámbitos*** de la ciberseguridad ***y de la protección de datos y de la intimidad***, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo; |

Or. en

*Justificación*

*Enmienda basada en el dictamen del SEPD. Las tareas de investigación de ENISA en el ámbito de la protección de datos y la intimidad figuraban en el anterior Reglamento 526/2013, pero ya no en la propuesta de la Comisión. La desaparición de esta labor de investigación y asesoramiento puede dar lugar a la interrupción de la labor de ENISA en materia de protección de datos y de la intimidad mejorando las tecnologías (PET) y, más en general, en materia de protección de datos desde el diseño y por defecto.*

**Enmienda 200**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 11 - párrafo 1 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) promoverá la colaboración multilateral en la regulación y la normalización para establecer unas condiciones equitativas que se ajusten al alcance global de la OMC;*** |

Or. en

**Enmienda 201**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 11 – párrafo 1 – letra c ter (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c ter) apoyará los esfuerzos para la inclusión de normas de ciberseguridad en los acuerdos comerciales;*** |

Or. en

**Enmienda 202**
**Jan Philipp Albrecht**

en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 13 – apartado 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y dos representantes nombrados por la Comisión. Todos los representantes tendrán derecho a voto. | 1. El Consejo de Administración estará integrado por un representante de cada Estado miembro***, tres representantes del Grupo Permanente de Partes Interesadas, uno de los cuales debe representar los intereses de los consumidores,*** y dos representantes nombrados por la Comisión. Todos los representantes tendrán derecho a voto. |

Or. en

*Justificación*

*La propuesta debe garantizar que los intereses de todas las partes interesadas están representados adecuadamente en la estructura de gobernanza de ENISA:*

**Enmienda 203**
**Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Marc Tarabella, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 13 – apartado 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y dos representantes nombrados por la Comisión. Todos los representantes tendrán derecho a voto. | 1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y dos representantes nombrados por la Comisión ***y el Parlamento Europeo***. Todos los representantes tendrán derecho a voto. |

Or. en

**Enmienda 204**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 14 – apartado 1 – letra e**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| e) evaluará y adoptará el informe anual consolidado sobre las actividades de la Agencia y, a más tardar el 1 de julio del año siguiente, remitirá dicho informe, junto con su evaluación, al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas; el informe anual incluirá las cuentas ***y*** describirá en qué medida la Agencia ha cumplido sus indicadores de rendimiento; el informe anual se hará público; | e) evaluará y adoptará el informe anual consolidado sobre las actividades de la Agencia y, a más tardar el 1 de julio del año siguiente, remitirá dicho informe, junto con su evaluación, al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas; el informe anual incluirá las cuentas***,*** describirá ***la utilidad de los recursos asignados y valorará*** en qué medida la Agencia ***ha sido eficaz y*** ha cumplido sus indicadores de rendimiento. el informe anual se hará público; |

Or. cs

**Enmienda 205**
**Maria Grapini**

**Propuesta de Reglamento**
**Artículo 14 – apartado 1 – letra m**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| m) nombrará al director ejecutivo y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 33 del presente Reglamento; | m) nombrará al director ejecutivo ***mediante una selección basada en criterios profesionales*** y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 33 del presente Reglamento; |

Or. ro

**Enmienda 206**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 14 – apartado 1 – letra o**

| *Texto de la Comisión* | *Enmienda* |
|---|---|

| | |
|---|---|
| o) adoptará todas las decisiones relativas al establecimiento de las estructuras internas de la Agencia y, cuando sea necesario, a su modificación, teniendo en cuenta las necesidades de la actividad de la Agencia, así como la buena gestión financiera; | o) adoptará todas las decisiones relativas al establecimiento de las estructuras internas de la Agencia y, cuando sea necesario, a su modificación, teniendo en cuenta las necesidades de la actividad de la Agencia, ***recogidas en el presente Reglamento,*** así como la buena gestión financiera; |

Or. cs

**Enmienda 207**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 18 – apartado 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3. El Comité Ejecutivo estará formado por cinco miembros escogidos entre los miembros del Consejo de Administración, entre los que figurarán el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y uno de los representantes de la Comisión. El director ejecutivo participará en las reuniones del Comité Ejecutivo, pero no tendrá derecho de voto. | 3. El Comité Ejecutivo estará formado por cinco miembros escogidos***, de una forma equilibrada desde el punto de vista del género,*** entre los miembros del Consejo de Administración, entre los que figurarán el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y uno de los representantes de la Comisión. El director ejecutivo participará en las reuniones del Comité Ejecutivo, pero no tendrá derecho de voto. |

Or. en

*Justificación*

*Debe introducirse la cuestión del equilibrio de género.*

**Enmienda 208**
**Evelyne Gebhardt, Kerstin Westphal, Lucy Anderson, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**

**Artículo 19 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. El director ejecutivo informará al Parlamento Europeo sobre el ejercicio de sus funciones cuando se le invite a hacerlo. El Consejo podrá convocar al director ejecutivo para que le informe sobre el ejercicio de sus funciones. | 2. El director ejecutivo informará al Parlamento Europeo ***anualmente*** sobre el ejercicio de sus funciones cuando se le invite a hacerlo. El Consejo podrá convocar al director ejecutivo para que le informe sobre el ejercicio de sus funciones. |

Or. en

**Enmienda 209**
**Arndt Kohn, Sergio Gutiérrez Prieto, Lucy Anderson, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 20 – apartado 1**

| *Texto de la Comisión* | *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, 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. | 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***, el Foro Europeo para la Acreditación, organismos de evaluación de la conformidad*** 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

**Enmienda 210**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 20 – apartado 1**

| *Texto de la Comisión* | *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, 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. | 1. El Consejo de Administración establecerá, a propuesta del director ejecutivo, un Grupo Permanente de Partes Interesadas integrado por expertos reconocidos ***en materia de seguridad*** que representen a las partes interesadas pertinentes, tales como la industria ***europea*** de las TIC, los proveedores ***europeos*** 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. |

Or. en

**Enmienda 211**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 20 – apartado 1**

| *Texto de la Comisión* | *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, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, los | 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 ***de la Unión***, los proveedores de redes o servicios de comunicaciones electrónicas ***de la Unión*** |

| | |
|---|---|
| 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. | 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. |

Or. en

**Enmienda 212**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 20 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. Los procedimientos del Grupo Permanente de Partes Interesadas, en particular con respecto al número, composición y nombramiento de sus miembros por el Consejo de Administración, a la propuesta por el director ejecutivo y al funcionamiento del Grupo, se especificarán en el reglamento operativo interno de la Agencia y se harán públicos. | 2. Los procedimientos del Grupo Permanente de Partes Interesadas, en particular con respecto al número, composición y nombramiento de sus miembros por el Consejo de Administración, a la propuesta por el director ejecutivo y al funcionamiento del Grupo, se especificarán en el reglamento operativo interno de la Agencia y se harán públicos. ***Los procedimientos seguirán las mejoras prácticas a la hora de garantizar una representación justa y una igualdad de derechos para todas las partes interesadas, y aplicarán un enfoque equilibrado desde el punto de vista del género.*** |

Or. en

*Justificación*

*Es necesaria una representación justa e igualitaria para conseguir los mejores resultados.*

**Enmienda 213**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 20 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. La composición del Grupo Permanente de Partes Interesadas incluirá un mínimo de cinco organizaciones de consumidores y organizaciones de la sociedad civil.*** |

Or. en

*Justificación*

*En el Grupo Permanente de Partes Interesadas actual, solo un experto de treinta del Grupo representa las opiniones de los consumidores, y eso no es suficiente.*

**Enmienda 214**
**Evelyne Gebhardt, Kerstin Westphal, Lucy Anderson, Marc Tarabella**

**Propuesta de Reglamento**
**Artículo 20 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. El mandato de los miembros del Grupo Permanente de Partes Interesadas tendrá una duración de dos años y medio. Los miembros del Consejo de Administración no podrán ser miembros del Grupo Permanente de Partes Interesadas. Los expertos de la Comisión y de los Estados miembros podrán estar presentes en las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos. Se podrá invitar a asistir a las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos a representantes de otros órganos que no sean miembros del mismo y el director ejecutivo considere | 4. El mandato de los miembros del Grupo Permanente de Partes Interesadas tendrá una duración de dos años y medio. Los miembros del Consejo de Administración ***y del Comité Ejecutivo, excepto el director ejecutivo mencionado en el apartado 3,*** no podrán ser miembros del Grupo Permanente de Partes Interesadas. Los expertos de la Comisión y de los Estados miembros podrán estar presentes en las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos. Se podrá invitar a asistir a las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos a representantes |

| | |
|---|---|
| pertinentes. | de otros órganos que no sean miembros del mismo y el director ejecutivo considere pertinentes. |
| | Or. en |

**Enmienda 215**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 20 – apartado 5**

| *Texto de la Comisión* | *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. | 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. ***También propondrá que la Comisión solicite a la Agencia preparar propuestas de regímenes europeos de certificación de la ciberseguridad de conformidad con el artículo 44, ya sea por propia iniciativa o tras la presentación de propuestas de las partes interesadas pertinentes.*** |
| | Or. en |

**Enmienda 216**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 20 – apartado 5**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 5. El Grupo Permanente de Partes Interesadas asesorará a la Agencia en lo relativo a la realización de sus actividades. | 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. | 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. ***Dará su aprobación formal a toda propuesta de régimen de certificación preparada por la Agencia antes de que se transmita a la Comisión Europea para su aprobación.*** |

Or. en

*Justificación*

*Validación obligatoria de una propuesta de régimen de certificación por parte del Grupo Permanente de Partes Interesadas de ENISA, que reúne a expertos en materia de ciberseguridad reconocidos como tales por el ecosistema de la ciberseguridad y académicos que garantizan una gobernanza justa y abierta.*

**Enmienda 217**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 20 – apartado 5 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***5 bis. El Grupo Permanente de Partes Interesadas se reunirá al menos cuatro veces al año. La orden del día para al menos una de esas reuniones se dedicará a los asuntos mencionados en los artículos 43 a 54 (título III).*** |

Or. en

**Enmienda 218**
**Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella**

**Propuesta de Reglamento**
**Artículo 20 – apartado 5 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***5 bis. Aconsejará a la Agencia cuando esta prepare las propuestas de regímenes.*** |

Or. en

**Enmienda 219**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 23 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. La Agencia velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 22. | 2. La Agencia velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a ***los debates y*** los resultados de su trabajo. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 22. |

Or. en

*Justificación*

*La transparencia debe ser ejecutable, teniendo en cuenta la aplicación del artículo 24.*

**Enmienda 220**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 34 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. El Consejo de Administración adoptará una decisión que establezca las normas aplicables a las comisiones de servicios de expertos nacionales en la | 2. El Consejo de Administración adoptará una decisión que establezca las normas aplicables a las comisiones de servicios de expertos nacionales en la |

| | |
|---|---|
| Agencia. | Agencia***, entre otras cosas, que deniegue las prácticas que impliquen costes nulos y que promueva una remuneración equitativa***. |

Or. en

*Justificación*

*Igualdad de retribución por un mismo trabajo: con el fin de conseguir el mejor personal, es inaceptable que la Unión exija a expertos de varios Estados miembros que trabajen con diferentes niveles salariales nacionales en las mismas tareas.*

**Enmienda 221**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 41 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. El Estado miembro que acoja a la Agencia ofrecerá las mejores condiciones posibles para garantizar su buen funcionamiento, incluida la accesibilidad de ***su*** ubicación, la presencia de servicios educativos adecuados para los hijos de los miembros del personal y un acceso adecuado al mercado de trabajo, la seguridad social y la atención médica para hijos y cónyuges. | 2. El Estado miembro que acoja a la Agencia ofrecerá las mejores condiciones posibles para garantizar su buen funcionamiento, incluida la accesibilidad de ***la sede y otra*** ubicación ***de las oficinas por aeropuerto internacional***, la presencia de servicios educativos adecuados para los hijos de los miembros del personal y un acceso adecuado al mercado de trabajo, la seguridad social y la atención médica para hijos y cónyuges. |

Or. en

*Justificación*

*Si bien el Estado anfitrión es una cuestión ajena al presente Reglamento, garantizar las mejores condiciones para que la Agencia funcione está dentro del ámbito de aplicación y, por ello, se proporciona orientación al respecto.*

**Enmienda 222**
**Philippe Juvin, Andreas Schwab**

**Propuesta de Reglamento**
**Artículo 43 – párrafo 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas. | ***Se creará*** un régimen europeo de certificación de la ciberseguridad ***a fin de reforzar el nivel de seguridad en el mercado único digital y adoptar un enfoque de la certificación europea armonizado a escala de la Unión, con vistas a garantizar productos, servicios y sistemas TIC resistentes a los ciberataques.***<br>***Dicho régimen*** confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos ***comunes*** especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas. |

Or. fr

**Enmienda 223**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 43 – párrafo 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para ***resistir, con un determinado nivel de garantía, las*** | Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados ***de conformidad con las normas*** en lo que respecta a su capacidad para ***cumplir los objetivos de seguridad*** |

| | |
|---|---|
| ***acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas***. | ***especificados***. |

Or. en

*Justificación*

*El régimen de certificación de la ciberseguridad debe tener un enfoque flexible, de acuerdo con el nivel de riesgos y los usos de un producto, servicio o proceso.*

**Enmienda 224**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 43 – párrafo 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas. | Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios ***de hardware y software*** de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía ***basada en los riesgos***, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos ***de hardware y software***, procesos ***de desarrollo y mantenimiento***, servicios y sistemas. |

Or. en

**Enmienda 225**

**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 43 – párrafo 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Un régimen europeo de certificación de la ciberseguridad confirmará que los productos ***y*** servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas. | Un régimen europeo de certificación de la ciberseguridad confirmará que los productos***,*** servicios ***y procesos*** de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos ***y las propiedades*** especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas. |

Or. en

**Enmienda 226**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 43 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***Artículo 43 bis*** |
| | ***Seguridad a través del diseño y por defecto*** |
| | ***1. Teniendo en cuenta el estado actual de la técnica, los productores y proveedores de servicios garantizarán la seguridad a través del diseño y por defecto de sus productos y servicios de TIC. Los fabricantes y proveedores de servicios deberán asegurarse de que el software que se ejecuta en su producto o servicio de TIC es seguro y no tiene ninguna*** |

***vulnerabilidad de seguridad conocida teniendo en cuenta la tecnología de vanguardia en el momento. Los productos y servicios de TIC deberán aplicar las siguientes medidas técnicas:***

***a) Los productos y servicios de TIC deberán estar dotados de software actualizado e incluir mecanismos para recibir actualizaciones de software seguras, debidamente autenticadas y fiables de forma regular;***

***b) las capacidades de acceso remoto del producto o servicio de TIC deberán estar documentadas y protegidas contra el acceso no autorizado durante la instalación a más tardar;***

***c) los productos de TIC no tendrán las mismas contraseñas estándar codificadas por hardware para todos los dispositivos;***

***d) los datos almacenados por los productos y servicios de TIC deberán estar protegidos de forma segura por los métodos más modernos, como el cifrado;***

***e) los productos y servicios de TIC solo aceptarán métodos de autenticación de alta seguridad.***

***2. Los fabricantes y los proveedores de servicios deberán notificar a la autoridad competente cualquier vulnerabilidad de seguridad conocida tan pronto como se descubra. Además, deberán ofrecer una reparación o sustitución oportuna para superar cualquier nueva vulnerabilidad de seguridad descubierta.***

***3. Los productos y servicios de TIC comercializados cumplirán las obligaciones establecidas en el apartado 1 durante su período de utilización previsible y normal.***

***4. La Comisión adoptará, mediante un acto de ejecución y en cooperación con ENISA, normas detalladas sobre las especificidades de los requisitos de***

***seguridad previstos en el apartado 1.***

***5. Cuando las autoridades de vigilancia del mercado tengan motivos para creer que el producto o servicio de TIC no cumple los requisitos establecidos en el presente Reglamento, exigirán sin demora al fabricante o proveedor de servicios correspondiente que adopte las medidas correctoras adecuadas para poner el producto en conformidad con dichos requisitos, retirarlo del mercado o recuperarlo en un plazo de tiempo razonable, proporcional a la naturaleza del riesgo, que ellas prescriban.***

***6. Si el fabricante o proveedor de servicios no adopta las medidas correctoras pertinentes en el plazo de tiempo indicado en el apartado 5, las autoridades de vigilancia del mercado tomarán las medidas provisionales adecuadas para prohibir o restringir la comercialización del producto en los mercados nacional, retirarlo del mercado o recuperarlo.***

***7. Las autoridades de vigilancia del mercado organizarán controles adecuados de la conformidad de los productos y obligarán a los fabricantes o proveedores de servicios a retirar del mercado los productos no conformes. Al identificar los productos que estarán sujetos a control de conformidad, las autoridades nacionales de certificación darán prioridad a los productos de alto riesgo para los consumidores, los productos integrados con nuevas tecnologías o los productos con altos índices de venta.***

Or. en

*Justificación*

*One of the key reasons behind the increase of cyberattacks is the lack of security functionalities incorporated in the design of the connected products and/or services. Today, most of the connected devices available in the EU's single market are designed and manufactured without the most basic security features embedded in their software. In order to trust the Internet of Things, consumers must be assured that the connected products they*

*purchase or services they use are secure and protected from software and hardware vulnerabilities. To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market. Such a horizontal and binding framework should be established as a complement of existing and pending legislation that requires cybersecurity measures such as the General Data Protection Regulation and the proposal for a European Electronic Communication Code.*

**Enmienda 227**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 43 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***Artículo 43 bis*** |
| | ***Plan de trabajo*** |
| | ***En consulta con el Comité de Consulta que se menciona en el artículo 44, la Comisión establecerá, a más tardar seis meses después de la entrada en vigor del Reglamento y luego cada dos años, un plan de trabajo que estará disponible públicamente.*** |

Or. en

*Justificación*

*La publicación del plan de trabajo mejorará la transparencia y la responsabilidad del desarrollo de los regímenes de certificación que se adopten a nivel de la Unión.*

**Enmienda 228**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Artículo 44 – apartado 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. ***Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de*** | 1. Los Estados miembros o el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») ***elaborarán*** |

| | |
|---|---|
| ***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. | un régimen europeo de certificación de la ciberseguridad ***que cumpla los requisitos fijados por esos mismos Estados miembros y expuestos en los artículos 45, 46 y 47 del presente Reglamento***. |

Or. fr

**Enmienda 229**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 44 – apartado 1**

| *Texto de la Comisión* | *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 ***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. | 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 Permanente de Partes Interesadas, ya se por iniciativa propia o tras la presentación de propuestas de las partes interesadas pertinentes, y*** 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. |

Or. en

**Enmienda 230**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 44 – apartado 1**

| *Texto de la Comisión* | *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 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.*** | 1. ***Los Estados miembros, el Grupo Permanente de Partes Interesadas establecido de conformidad con el artículo 20 o un organismo representante de la industria podrán proponer a la Comisión o al Grupo Europeo de Certificación de la Ciberseguridad (el «Grupo») la preparación de un régimen europeo de certificación de la ciberseguridad.*** Tras recibir una solicitud de la Comisión ***o del Grupo***, 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. |

Or. en

**Enmienda 231**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 44 – apartado 1**

| *Texto de la Comisión* | *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 ***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. | 1. Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de certificación de la ***seguridad informática*** 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 establecido con arreglo al artículo 20*** podrán proponer a la Comisión la preparación de un régimen europeo de certificación de la ciberseguridad. |

*Justificación*

*Es de suma importancia que todos los expertos sean consultados sistemática y regularmente durante la preparación de un régimen de certificación en ENISA.*

**Enmienda 232**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 44 – apartado 1 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis. Con el apoyo de la Comisión Europea y de los Estados miembros, ENISA creará un Comité de Consulta con una participación equilibrada del Grupo Europeo de Certificación de la Ciberseguridad y de todas las partes interesadas, como la industria, incluidas las pymes, los sindicatos, las organizaciones de desarrollo de normas, los comerciantes, los minoristas, los importadores o los consumidores finales, interesados en el producto, proceso o servicio de TIC de que se trate.*** |
| | ***Este Comité participará en cada fase de la preparación de una propuesta de régimen europeo de certificación de la ciberseguridad, incluida la definición de sus elementos y requisitos de garantía. El Comité de Consulta será consultado al menos una vez antes de la elaboración de una propuesta de régimen, al menos una vez cuando se disponga del primer proyecto de la propuesta de régimen, y antes de la adopción de las medidas de ejecución. El Comité de Consulta puede presentar una solicitud a ENISA para la preparación de una propuesta de régimen europeo de certificación de la ciberseguridad, que incluya iniciativas lideradas por la industria.*** |

Or. en

**Enmienda 233**
**Catherine Stihler, Liisa Jaakonsaari, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 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. ***ENISA garantizará la participación de los representantes de los Estados miembros y de todas las partes interesadas importantes implicadas en el grupo de productos o servicio de TIC de que se trate. Esto incluye partes a lo largo de las cadenas de valor, tales como sindicatos, comerciantes, minoristas, importadores, organismos de evaluación de la conformidad, usuarios finales y otros. Las partes interesadas empresariales también implicadas incluyen, entre otros: fabricantes, proveedores de soluciones de ciberseguridad, integradores de sistemas, profesionales de la seguridad y propietarios de activos.*** |

Or. en

**Enmienda 234**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 2. ***Mediante la preparación de*** 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. ***Las partes interesadas pertinentes y*** 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

**Enmienda 235**
**Roberta Metsola, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 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 ***a la hora de definir los objetivos de seguridad de la propuesta de régimen de certificación en línea con el artículo 45, lo que dará lugar a la elaboración de una lista de control de los riesgos y las correspondientes características de ciberseguridad***. 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.

Or. en

**Enmienda 236**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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***. | 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 la partes interesadas ***restantes en un proceso formal, normalizado y transparente,*** y cooperará estrechamente con el Grupo. El Grupo ***y las partes interesadas restantes pertinentes facilitarán*** a ENISA la asistencia y el asesoramiento experto en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes. |

Or. en

**Enmienda 237**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 | 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 ***en un proceso formal, normalizado y transparente*** y cooperará estrechamente con el Grupo. El |

| | |
|---|---|
| asesoramiento experto que requiera en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes en caso necesario. | Grupo ***y las partes interesadas restantes pertinentes facilitarán*** 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. |

Or. en

**Enmienda 238**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 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***, así como con las organizaciones de consumidores y con el Grupo de trabajo del artículo 29 y el Comité Europeo de Protección de Dato***s. 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. |

Or. en

*Justificación*

*Enmienda basada en el dictamen del SEPD. La creación de sinergias técnicas y en materia de gobernanza reviste la máxima importancia para que las certificaciones con arreglo al marco europeo de certificación de la ciberseguridad y al Reglamento general de protección de datos no sean percibidas como contradictorias o carentes de relación por las organizaciones que luchan por la aplicación de los instrumentos pertinentes.*

**Enmienda 239**

**Lucy Anderson, Sergio Gutiérrez Prieto, Kerstin Westphal, Marc Tarabella, Christel Schaldemose, Liisa Jaakonsaari**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 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***, incluidos los representantes pertinentes de la sociedad civil como las organizaciones de consumidores,*** 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. |

Or. en

**Enmienda 240**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ***ENISA tendrá en cuenta las normas nacionales e internacionales ya existentes.*** 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. |

Or. en

**Enmienda 241**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ENISA consultará ***al Comité de Consulta y*** 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. |

Or. en

**Enmienda 242**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | 2. A la hora de preparar las propuestas de régimen, 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. |

Or. fr

**Enmienda 243**
**Roberta Metsola, Lara Comi, Pascal Arimont, Andreas Schwab, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. ENISA coordinará la elaboración de una lista de control de los riesgos asociados con el hardware o software del producto o servicio de TIC: Los riesgos se corresponderán con las características de ciberseguridad correspondientes que se incluirán en la propuesta de régimen europeo de certificación de la ciberseguridad.*** |

Or. en

**Enmienda 244**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. El marco de certificación se beneficiará de los conocimientos técnicos y la experiencia de los Estados miembros con un historial importante en estas cuestiones estratégicas, con el apoyo de las industrias que hayan adquirido una experiencia significativa en la materia.*** |

Or. fr

**Enmienda 245**
**Catherine Stihler, Liisa Jaakonsaari**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. ENISA tratará de ajustar en la mayor medida posible cualquier propuesta de régimen de certificación de ciberseguridad, elaborada de conformidad con el apartado 1 del presente artículo, a las normas pertinentes reconocidas internacionalmente.*** |

Or. en

**Enmienda 246**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. ENISA respetará el secreto profesional con respecto a toda la información obtenida a la hora de llevar a cabo sus tareas en virtud del presente Reglamento.*** |

Or. en

**Enmienda 247**
**Roberta Metsola, Lara Comi, Pascal Arimont, Andreas Schwab, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 44 – apartado 2 ter (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 ter. La lista de control preparada se basará en la experiencia de los Estados miembros en la elaboración y aplicación de certificados de ciberseguridad en sus jurisdicciones respectivas. Se elaborará una lista de los riesgos previstos, que se analizará y, dependerá de una evaluación del entorno de riesgo en el que funcionará el producto de hardware o software de*** |

***TIC o el servicio de TIC, así como del usuario final previsto.***

Or. en

*Justificación*

*La lista de control aclarará exactamente qué riesgos específicos podrá soportar, por su diseño, el producto o servicio, e incluirá las características de ciberseguridad correspondientes. El nivel del certificado según lo indicado en el artículo 46 asignado dependerá del número de riesgos que aborde el certificado. La lista de control ayudará a diferenciar los enfoques según el producto o servicio, desde un dispositivo de la internet de las cosas pequeño y personal hasta una gestión sofisticada de las instalaciones en sectores sensibles.*

**Enmienda 248**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 44 – apartado 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3. ***ENISA*** transmitirá a la Comisión la propuesta de régimen ***europeo de certificación de la ciberseguridad*** preparada de conformidad con el apartado 2 del presente artículo. | 3. ***Previa aprobación del Grupo de la propuesta de régimen europeo de certificación de la seguridad,*** ENISA***, tras consultar con el Grupo Permanente de Partes Interesadas,*** transmitirá a la Comisión la propuesta de régimen preparada de conformidad con el apartado 2 del presente artículo. |

Or. en

**Enmienda 249**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Artículo 44 – apartado 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3. ENISA transmitirá a la Comisión ***la propuesta de*** régimen europeo de | 3. ENISA transmitirá a la Comisión ***el*** régimen europeo de certificación de la |

certificación de la ciberseguridad ***preparada*** de conformidad con el apartado 2 del presente artículo.

ciberseguridad ***adoptado en último término por los Estados miembros*** de conformidad con el apartado 2 del presente artículo.

Or. fr

**Enmienda 250**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 44 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Comisión***,*** sobre ***la base de*** la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. | 4. La Comisión ***consultará a todas las partes interesadas pertinentes*** sobre la propuesta de régimen preparada por ENISA***, y evaluará su adecuación para cumplir los objetivos de la solicitud y si el régimen contribuye a un alto nivel de protección de los consumidores y usuarios finales y a la competitividad europea. Tras una consulta y una evaluación, la Comisión*** podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. |

Or. en

**Enmienda 251**
**Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 44 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Comisión***, sobre la base de la*** | 4. La Comisión ***tendrá la facultad*** |

| | |
|---|---|
| ***propuesta de régimen preparada por ENISA, podrá*** adoptar actos ***de ejecución***, de conformidad con el artículo 55***, apartado 1, que establezcan*** regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. | ***para*** adoptar actos ***delegados***, de conformidad con el artículo 55 ***bis, en relación con el establecimiento de*** regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. ***A la hora de adoptar estos actos delegados, la Comisión se basará en los regímenes de certificación de la ciberseguridad para productos y servicios de TIC o en propuestas de regímenes relevantes que proponga ENISA.*** |

Or. en

*Justificación*

*Dado que la Comisión debe establecer un número significativo de normas sobre cuestiones tales como el ámbito de aplicación de cada régimen de certificación, los requisitos aplicables, las normas de control, etc., es jurídicamente más adecuado adoptar regímenes de certificación mediante actos delegados.*

**Enmienda 252**
**Jan Philipp Albrecht**
en nombre del Grupo Verts/ALE

**Propuesta de Reglamento**
**Artículo 44 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. | 4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. ***La Comisión podrá consultar al Comité Europeo de Protección de Datos y tener en cuenta su punto de vista antes de la adopción de dichos actos de ejecución.*** |

Or. en

*Justificación*

*Enmienda basada en el dictamen del SEPD. La presente enmienda garantiza la coherencia entre las certificaciones con arreglo al marco europeo de certificación de la ciberseguridad y al Reglamento general de protección de datos.*

**Enmienda 253**
**Mylène Troszczynski**

**Propuesta de Reglamento**
**Artículo 44 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Comisión, sobre la base ***de la propuesta de*** régimen ***preparada*** por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. | 4. La Comisión, sobre la base ***del*** régimen ***de certificación comunicado*** por ENISA ***y adoptado por los Estados miembros***, podrá adoptar ***posteriormente*** actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. |

Or. fr

**Enmienda 254**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 44 – apartado 4**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios | 4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios |

| | |
|---|---|
| de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. | ***de hardware y software*** de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento. |

Or. en

**Enmienda 255**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 44 – apartado 5**

| *Texto de la Comisión* | *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. | 5. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los regímenes europeos de certificación de la ciberseguridad y darles publicidad***, así como sobre las propuestas de regímenes europeos de certificación de la ciberseguridad y darles publicidad en preparación***. |

Or. en

**Enmienda 256**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 44 – apartado 5 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***5 bis. ENISA requiere una oficina en Bruselas que supervise de cerca el trabajo sobre la certificación de la Unión y que trabaje en estrecho contacto con la Comisión y el Parlamento para establecer normas europeas comunes en materia de ciberseguridad.*** |

Or. en

**Enmienda 257**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 44 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***Artículo 44 bis*** |
| | ***Programa de trabajo*** |
| | ***1. Previa consulta al Grupo y al Grupo Permanente de Partes Interesadas, ENISA, como complemento o como parte de su programa general de trabajo, previa aprobación de la Comisión y, en cualquier caso, a más tardar el ... [seis meses después de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, cada dos años, establecerá un plan de trabajo para el desarrollo de regímenes europeos de certificación de la ciberseguridad, que estará disponible públicamente.*** |
| | ***Los planes de trabajo establecerán, para los dos años siguientes, una lista indicativa de productos, procesos y servicios considerados prioritarios para la adopción de regímenes europeos de certificación de la ciberseguridad. El plan de trabajo será modificado por ENISA, en su caso, previa consulta a la Comisión, al Grupo y al Grupo Permanente de Partes Interesadas, con el fin de tener en cuenta, entre otras cosas, las exigencias del mercado interior.*** |

Or. en

**Enmienda 258**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|

| | |
|---|---|
| Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, según proceda, ***los siguientes*** objetivos de seguridad: | Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, según proceda, ***la siguiente lista no exhaustiva*** de objetivos de seguridad: |

Or. en

**Enmienda 259**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, ***según proceda***, los siguientes objetivos de seguridad: | Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, ***al menos***, los siguientes objetivos de seguridad***, en la medida en que sean pertinentes***: |

Or. en

**Enmienda 260**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse ***para tener*** en cuenta, según proceda, los siguientes objetivos de seguridad: | Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse ***de tal forma que tengan*** en cuenta, según proceda, los siguientes objetivos de seguridad: |

Or. en

**Enmienda 261**
**Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – parte introductoria**

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

Or. fr

**Enmienda 262**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) proteger los datos almacenados, transmitidos o procesados de otro modo frente al almacenamiento, procesamiento, acceso o revelación accidentales o no autorizados; | a) ***Confidencialidad:*** proteger los datos almacenados, transmitidos o procesados de otro modo frente al almacenamiento, procesamiento, acceso o revelación accidentales o no autorizados; |

Or. en

**Enmienda 263**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) proteger los datos almacenados, transmitidos o procesados de otro modo frente a la destrucción accidental o no autorizada, la pérdida accidental o la alteración; | b) ***Integridad:*** proteger los datos almacenados, transmitidos o procesados de otro modo frente a la destrucción accidental o no autorizada, la pérdida accidental o la alteración; |

Or. en

**Enmienda 264**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***c) garantizar que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso;*** | ***suprimida*** |

Or. en

**Enmienda 265**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 45 - párrafo 1 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) proteger y asegurar los dispositivos contra la suplantación de identidad y otras formas de imitación de dispositivos;*** |

Or. en

**Enmienda 266**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra d**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***d) registrar qué datos, funciones o servicios se han comunicado, en qué momentos y por quién;*** | ***suprimida*** |

Or. en

**Enmienda 267**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra e**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***e) garantizar que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso o de uso, en qué momentos y por quién;*** | ***suprimida*** |

Or. en

**Enmienda 268**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra f**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| f) ***restaurar la*** disponibilidad ***y el acceso a*** los datos, servicios y funciones ***de forma rápida en caso de incidente físico o técnico***; | f) Disponibilidad : ***promover la accesibilidad de*** los datos, servicios y funciones ***por parte de los usuarios autorizados***; |

Or. en

**Enmienda 269**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | g) garantizar que los productos y servicios de TIC se entreguen siempre con un software actualizado, que no contenga vulnerabilidades conocidas ***críticas para la garantía ofrecida por el régimen, se hayan diseñado y ejecutado de manera que limiten de forma eficaz la inclusión o*** |

***introducción de vulnerabilidades,*** y dispongan de mecanismos para efectuar actualizaciones de seguridad del software

Or. en

**Enmienda 270**
**Andreas Schwab**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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***. | g) garantizar que los productos y servicios de TIC se entreguen siempre con ***actualizaciones, mejoras y parches***, que no ***contengan*** vulnerabilidades conocidas, y ***que se ofrezcan durante un ciclo de vida razonable del producto o servicio con el fin de permitir una protección continua***. |

Or. en

**Enmienda 271**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra g**

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

Or. en

**Enmienda 272**
**Roberta Metsola, Eva Maydell, Lara Comi, Pascal Arimont, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | g) garantizar que los productos y servicios ***de hardware y software 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. |

Or. en

**Enmienda 273**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 45 – párrafo 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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. | g) garantizar que los productos y servicios de TIC se entreguen siempre con un software actualizado, que no contenga vulnerabilidades ***ni lagunas*** conocidas, y dispongan de mecanismos para efectuar actualizaciones de seguridad del software. |

Or. cs

**Enmienda 274**
**Dita Charanzová, Morten Løkkegaard**

**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 desarrollen y*** |

***funcionen de conformidad con las normas y políticas de seguridad adecuadas y que el nivel más elevado de ciberseguridad y protección de datos esté preconfigurado por defecto en los productos, servicios y procesos.***

Or. en

**Enmienda 275**
**Catherine Stihler, Liisa Jaakonsaari, Christel Schaldemose, Arndt Kohn, Lucy Anderson**

**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», siguiendo un enfoque basado en el riesgo en función del contexto y la gravedad de la situación tal y como se define en el artículo 46.*** |

Or. en

**Enmienda 276**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 46 – título**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Niveles de garantía de los regímenes europeos de certificación de la ciberseguridad | Niveles de garantía ***basados en el riesgo*** de los regímenes europeos de certificación de la ciberseguridad |

Or. en

**Enmienda 277**

**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 46 – título**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***Niveles de garantía*** de los regímenes europeos de certificación de la ciberseguridad | ***Objetivos de seguridad*** de los regímenes europeos de certificación de la ciberseguridad |

Or. en

**Enmienda 278**
**Anneleen Van Bossuyt, Daniel Dalton**

**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 TIC amparados en dicho régimen. | 1. Un régimen europeo de certificación de la ciberseguridad podrá especificar ***distintos*** niveles de garantía para los productos y servicios de TIC amparados en dicho régimen. ***Dichos niveles se distinguirán en función del grado de confianza en las cualidades de ciberseguridad alegadas o afirmadas de un producto o servicio de TIC, caracterizadas con referencia a las normas y procedimientos correspondientes, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad.*** |

Or. en

**Enmienda 279**
**Antanas Guoga**

**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 TIC amparados en dicho régimen***. | 1. ***En consulta con las partes interesadas pertinentes, ENISA identificará o desarrollará los niveles de garantía que se especificarán en los regímenes europeos*** de certificación de la ciberseguridad. |

Or. en

**Enmienda 280**
**Jiří Maštálka**

**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 TIC amparados en dicho régimen***. | 1. Un régimen europeo de certificación de la ciberseguridad podrá especificar uno o más ***requisitos*** de garantía ***sobre la base del riesgo y las amenazadas determinadas por el contexto en el que se opera el producto, proceso o servicio***. |

Or. en

**Enmienda 281**
**Andreas Schwab, Philippe Juvin**

**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 TIC amparados en dicho régimen. | 1. Un régimen europeo de certificación de la ciberseguridad podrá especificar uno o más de los siguientes ***requisitos de seguridad***: básico, sustancial y/o elevado, para los productos y servicios de TIC amparados en dicho régimen. ***Los requisitos de seguridad se definirán siguiendo un enfoque basado en el riesgo*** |

***y teniendo en cuenta el uso previsto del producto o servicio de TIC.***

Or. en

**Enmienda 282**
**Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Kerstin Westphal, Pina Picierno, Marc Tarabella, Christel Schaldemose**

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

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 su riesgo inherente, y no los productos y servicios de TIC en sí.*

**Enmienda 283**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 46 – apartado 1**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. ***Un*** régimen europeo de certificación de la ciberseguridad podrá | 1. ***Todo*** 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 TIC*** amparados en dicho régimen. | especificar uno o más de los siguientes niveles de garantía: ***«funcionalmente seguro», «sustancialmente seguro» y/o «extremadamente seguro», para los certificados de ciberseguridad*** amparados en dicho régimen***, teniendo en cuenta, entre otros factores, el uso previsto de los mismos***. |

Or. en

**Enmienda 284**
**Roberta Metsola, Lara Comi**

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

Or. en

**Enmienda 285**
**Jiří Pospíšil**

**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 TIC amparados en dicho régimen. | *(No afecta a la versión española.)* |

Or. cs

**Enmienda 286**
**Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Pina Picierno, Marc Tarabella, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 46 – apartado 1 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis. Todo régimen indicará la metodología o el proceso de evaluación que deba seguirse para expedir certificados a cada nivel de garantía, en función del uso previsto y del riesgo inherente a los productos y servicios de TIC amparados en dicho régimen.*** |

Or. en

*Justificación*

*Para evitar la fragmentación entre los Estados miembros de la Unión, debe asociarse a cada nivel de garantía una metodología o un procedimiento de evaluación armonizado.*

**Enmienda 287**
**Roberta Metsola, Lara Comi, Andreas Schwab, Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 46 – apartado 1 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis. Un régimen europeo de certificación de la ciberseguridad especificará si está permitida la autodeclaración de conformidad o si es estrictamente necesaria la evaluación por parte de terceros.*** |

Or. en

**Enmienda 288**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***2. Los niveles de garantía básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente:*** | ***suprimido*** |
| ***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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;*** | |
| ***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;*** | |
| ***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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.*** | |

**Enmienda 289**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***2. Los niveles de garantía básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente:*** | ***suprimido*** |
| ***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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;*** | |
| ***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;*** | |
| ***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 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 290**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. ***Los niveles de garantía básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente:*** | 2. ***Un régimen europeo de certificación de la ciberseguridad especificará si está permitida la autodeclaración de conformidad o si es necesaria la evaluación por parte de terceros.*** |

Or. en

*Justificación*

*Los regímenes de certificación de la ciberseguridad deben tener un enfoque flexible, de acuerdo con el nivel de riesgos y los usos de un producto, servicio o proceso. Hemos de reaccionar ante un entorno que cambia rápidamente.*

**Enmienda 291**
**Roberta Metsola, Eva Maydell, Lara Comi**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. Los niveles de garantía ***básico***, sustancial y elevado cumplirán los siguientes criterios, respectivamente: | 2. Los niveles de garantía***, basados en el riesgo, elemental***, sustancial y elevado cumplirán los siguientes criterios, respectivamente: |

Or. en

**Enmienda 292**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. Los ***niveles de garantía*** básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente: | 2. Los ***requisitos de seguridad*** básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente: |

Or. en

**Enmienda 293**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;*** | ***suprimida*** |

Or. en

**Enmienda 294**
**Antanas Guoga**

**Propuesta de Reglamento**

**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;*** | ***suprimida*** |

Or. en

**Enmienda 295**
**Arndt Kohn, Evelyne Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;*** | a) el nivel de garantía ***«funcionalmente seguro» estará relacionado con un riesgo bajo*** de un producto ***y*** servicio de TIC***. Existe un bajo nivel de riesgo cuando un ataque al producto y servicio de TIC no compromete la confidencialidad, integridad, disponibilidad, privacidad u otros objetivos importantes, ni la salud de los usuarios o terceros, el medio ambiente, otros intereses legítimos importantes o la infraestructura crítica y sus sistemas o productos de apoyo.*** |

Or. en

**Enmienda 296**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad; | 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 conexos, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad; ***cuando un régimen europeo de certificación de la ciberseguridad incluya la certificación de un proceso de ciberseguridad por un fabricante, esa certificación de un proceso de ciberseguridad podrá incluir la concesión de un permiso al fabricante para la autodeclaración de la conformidad de los productos o servicios de TIC con el nivel de garantía «funcionalmente seguro»;*** |

Or. en

**Enmienda 297**
**Roberta Metsola, Lara Comi**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 | a) el nivel de garantía ***elemental*** se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado ***mínimo esencial*** de confianza ***y seguridad en caso de amenazas comunes a la ciberseguridad a*** |

| | |
|---|---|
| caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad; | ***que se enfrentan predominantemente los productos de consumo*** 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 el riesgo de incidentes de ciberseguridad; |

Or. en

**Enmienda 298**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad; | a) el ***requisito de seguridad*** 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, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad; |

Or. en

**Enmienda 299**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***b) el nivel de garantía sustancial se*** | ***suprimida*** |

***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 300**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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;*** | ***suprimida*** |

Or. en

**Enmienda 301**
**Arndt Kohn, Evelyne Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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;*** | b) el nivel de garantía ***«sustancialmente seguro» estará relacionado con un riesgo bajo*** de un producto ***y*** servicio de TIC***. Existe un nivel superior de riesgo cuando un ataque al producto y servicio de TIC compromete la confidencialidad, integridad, disponibilidad, privacidad u otros objetivos importantes, y repercute en la salud de los usuarios o terceros, el medioambiente, otros intereses legítimos importantes o la infraestructura crítica y sus sistemas o productos de apoyo.*** |

Or. en

**Enmienda 302**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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; | b) el nivel de garantía sustancial ***basado en el riesgo*** 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 ***que por lo general se usan a nivel industrial***, cuyo objeto es reducir sustancialmente el riesgo de incidentes de ciberseguridad; |

Or. en

**Enmienda 303**

**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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; | b) el ***requisito de seguridad*** 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; |

Or. en

**Enmienda 304**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.*** | ***suprimida*** |

Or. en

**Enmienda 305**
**Jiří Maštálka**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.*** | ***suprimida*** |

Or. en

**Enmienda 306**
**Arndt Kohn, Evelyne Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los*** | c) el nivel de garantía ***«extremadamente seguro» estará relacionado con un riesgo elevado de un producto y servicio. Existe un nivel elevado de riesgo cuando un ataque a*** un producto ***y*** servicio de TIC ***compromete la confidencialidad, integridad, disponibilidad, privacidad u otros objetivos importantes y pone razonablemente en peligro la soberanía nacional o la seguridad pública de los Estados***. |

***controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad***.

Or. en

**Enmienda 307**
**Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. | 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. ***Este nivel de garantía no deberá sugerir una seguridad absoluta para no inducir a error al usuario final.*** |

Or. en

**Enmienda 308**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 | c) el ***requisito de seguridad*** 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. | cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC superior al de los certificados con ***requisito de seguridad*** sustancial, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. ***Esto se aplicará en particular a los productos y servicios de infraestructuras críticas.*** |

Or. en

**Enmienda 309**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. | c) el nivel de garantía ***basado en el riesgo*** 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos ***que por lo general se usan a nivel industria***, cuyo objetivo es evitar los incidentes de ciberseguridad. |

Or. en

**Enmienda 310**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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 caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad. | 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 ***«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 311**
**Roberta Metsola, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. El nivel de garantía basado en el riesgo para una propuesta de régimen europeo de certificación de la ciberseguridad se determinará en función de los riesgos identificados en la lista de control establecida en el artículo 44, apartado 2, y de la disponibilidad de medidas de ciberseguridad para contrarrestar esos riesgos en el hardware y software de los productos de TIC a los que se aplique el régimen de certificación.*** |

Or. en

*Justificación*

*La lista de control aclarará qué riesgos específicos podrá soportar, por su diseño, el*

*producto o servicio, e incluirá las características de ciberseguridad correspondientes. El nivel del certificado según lo indicado en el artículo 46 asignado dependerá del número de riesgos que aborde el certificado. La lista de control ayudará a diferenciar los enfoques según el producto o servicio, desde un dispositivo de la internet de las cosas pequeño y personal hasta una gestión sofisticada de las instalaciones en sectores sensibles.*

**Enmienda 312**
**Philippe Juvin, Andreas Schwab**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 bis. Por lo que respecta a los niveles de garantía «sustancialmente seguro» y «extremadamente seguro», los organismos nacionales de control de la conformidad podrán utilizar el método del «hacking ético».*** |

Or. fr

**Enmienda 313**
**Roberta Metsola, Lara Comi, Antonio López-Istúriz White, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 46 – apartado 2 ter (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***2 ter. Las características identificadas en el nivel de garantía basado en el riesgo elemental del artículo 46, apartado 2, son las medidas mínimas de ciberseguridad aceptables para los productos de consumo. Las características identificadas en los niveles de garantía basados en el riesgo sustancial y elevado son las medidas mínimas de ciberseguridad aceptables para los productos y servicios de hardware y software de TIC utilizados a escala industrial. Estas características generales no deberían restringir a ENISA, previa consulta con los Estados*** |

***miembros y con el Grupo Permanente de Partes Interesadas, la elección de un nivel de garantía basado en el riesgo superior al estrictamente necesario tras una evaluación exhaustiva.***

Or. en

*Justificación*

*Esta disposición permitirá la flexibilidad en los casos en que los Estados miembros dispongan de regímenes existentes (que deberán ser sustituidos por un régimen europeo de ciberseguridad una vez que expiren) que ofrezcan más ciberseguridad de la que se prevé que ofrecerá la propuesta de régimen que prepara ENISA.*

**Enmienda 314**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – título**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| Elementos de los regímenes europeos ***de certificación*** de ***la*** ciberseguridad | Elementos de los regímenes europeos de ciberseguridad |

Or. en

*Justificación*

*La enmienda anterior es necesaria para garantizar que las actualizaciones no desencadenen automáticamente procedimientos de reevaluación o notificación. Exigir a las entidades que se sometan a evaluaciones de la conformidad repetidas cada vez que se realice un cambio (incluso en el caso de cambios que mejoren la seguridad o que solo afecten a la usabilidad o al rendimiento) limitaría en gran medida el atractivo y el éxito del marco de la Unión propuesto (y podría crear incluso desincentivos perjudiciales contra las actualizaciones oportunas para abordar las vulnerabilidades identificadas).*

**Enmienda 315**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. Un régimen europeo de certificación de la ciberseguridad ***incluirá los siguientes elementos***: | 1. ***Se deberá considerar lo siguiente a la hora de preparar*** un régimen europeo de certificación de la ciberseguridad: |

Or. en

**Enmienda 316**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. Un régimen europeo de certificación de la ciberseguridad incluirá los siguientes elementos: | 1. Un régimen europeo de certificación de la ciberseguridad incluirá ***uno o más de*** los siguientes elementos: |

Or. en

**Enmienda 317**
**Roberta Metsola, Lara Comi, Eva Maydell, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. Un régimen europeo de certificación de la ciberseguridad incluirá los siguientes elementos: | 1. Un régimen europeo de certificación de la ciberseguridad incluirá***, al menos,*** los siguientes elementos: |

Or. en

**Enmienda 318**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – parte introductoria**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 1. Un régimen europeo ***de certificación*** de ***la*** ciberseguridad incluirá los siguientes elementos: | 1. Un régimen europeo de ciberseguridad incluirá los siguientes elementos: |

Or. en

**Enmienda 319**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) objeto y alcance de ***la*** certificación, incluido el tipo o categoría de productos y servicios de TIC cubiertos; | a) objeto y alcance ***del régimen*** de certificación, incluido el tipo o categoría de productos***, procesos*** y servicios de TIC cubiertos***, siendo esta certificación específica de uno o más sectores o aplicándose de forma horizontal***; |

Or. en

**Enmienda 320**
**Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra a**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| a) objeto y alcance de la certificación, incluido el tipo o categoría de productos y servicios de TIC cubiertos; | a) objeto y alcance de la certificación, incluido el tipo o categoría de productos y servicios ***de hardware y software*** de TIC cubiertos; |

Or. en

**Enmienda 321**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, ***por ejemplo*** haciendo referencia a normas o especificaciones técnicas internacionales o ***de la Unión***; | b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, haciendo referencia a normas o especificaciones técnicas internacionales***, europeas o nacionales seguidas en el proceso de evaluación y certificación***; |

Or. en

**Enmienda 322**
**Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o de la Unión; | b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos ***de hardware y software*** de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o de la Unión; |

Or. en

**Enmienda 323**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y | b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y |

| | |
|---|---|
| productos de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o ***de la Unión***; | productos de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o ***europeas***; |

Or. en

**Enmienda 324**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, ***por ejemplo*** haciendo referencia a normas o especificaciones técnicas internacionales ***o de la Unión***; | b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, haciendo ***especial*** referencia a normas o especificaciones técnicas internacionales; |

Or. en

**Enmienda 325**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***b bis) especificación detallada si una certificación concedida solo puede aplicarse a un producto individual o a una gama de productos (diferentes versiones/modelos de la misma estructura de producto base);*** |

Or. en

**Enmienda 326**
**Antanas Guoga**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra b bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***b bis) pertinencia de promover la «seguridad a través del diseño»;*** |

Or. en

**Enmienda 327**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| c) en su caso, uno o varios niveles de garantía; | c) en su caso, uno o varios niveles de garantía ***basados en el riesgo***; |

Or. en

**Enmienda 328**
**Andreas Schwab, Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra c**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| c) en su caso, uno o varios ***niveles de garantía***; | c) en su caso, uno o varios ***requisitos de seguridad***; |

Or. en

**Enmienda 329**
**Roberta Metsola, Eva Maydell, Lara Comi, Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 47 - apartado 1 - letra c bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c bis) el procedimiento aplicable de evaluación de la conformidad o la autodeclaración de conformidad;*** |

Or. en

**Enmienda 330**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra c ter (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***c ter) los requisitos de certificación definidos de manera que la certificación pueda incorporarse o basarse en los procesos sistemáticos de ciberseguridad del productor seguidos durante el diseño, desarrollo y ciclo de vida del producto o servicio de TIC;*** |

Or. en

**Enmienda 331**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra e**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| e) información necesaria para la certificación que deben facilitar los solicitantes a los organismos de evaluación de la conformidad; | e) ***en relación con la opción de certificación del régimen por parte de terceros mencionada en el artículo 47 bis, apartado 2, letra b),*** información necesaria para la certificación que deben facilitar los solicitantes a los organismos de evaluación de la conformidad; |

Or. en

**Enmienda 332**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra f**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***f) cuando el régimen prevea marcas o etiquetas, las condiciones en las que pueden utilizarse tales marcas o etiquetas;*** | ***suprimida*** |

Or. en

**Enmienda 333**
**Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra f**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| f) cuando el régimen prevea marcas o etiquetas, las condiciones en las que pueden utilizarse tales marcas o etiquetas; | f) cuando el régimen prevea marcas o etiquetas***, como una Etiqueta de conformidad de ciberseguridad de la Unión que signifique que el producto o servicio de TIC es conforme con los criterios de un régimen europeo de certificación de la ciberseguridad,*** las condiciones en las que pueden utilizarse tales marcas o etiquetas |

Or. en

*Justificación*

*Hemos de garantizar que facilitamos a los ciudadanos información objetiva sobre la que puedan tomar decisiones con conocimiento de causa. No se debe hacer creer a los ciudadanos que un producto está libre de riesgos, puesto que esto es técnicamente inalcanzable y podría dar lugar a una reacción negativa contra la Unión. En la etiqueta del producto o servicio debe indicarse claramente que dicho producto o servicio cumple un régimen europeo de certificación de la ciberseguridad y el nivel de garantía basado en el riesgo que le corresponde.*

**Enmienda 334**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***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;*** | ***suprimida*** |

Or. en

**Enmienda 335**
**Andreas Schwab**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra g**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 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; | 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***, cuando proceda y sea posible también mediante actualizaciones, mejoras o parches obligatorios del producto o servicio de TIC de que se trate. Para todos los productos y servicios de TIC con requisitos de seguridad sustanciales y elevados, la vigilancia será obligatoria con regularidad***; |

Or. en

**Enmienda 336**

**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra g**

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

Or. en

**Enmienda 337**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra h**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***h) condiciones para la concesión, el mantenimiento, la continuación, la ampliación y la reducción del alcance de la certificación;*** | ***suprimida*** |

Or. en

**Enmienda 338**
**Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra h**

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

Or. fr

**Enmienda 339**
**Lucy Anderson, Marc Tarabella, Christel Schaldemose, Liisa Jaakonsaari**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra h bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***h bis) El régimen de certificación especificará las condiciones para la nueva certificación o la evaluación de un producto o servicio. Esto es de particular importancia para los servicios de software que poseen características de seguridad y actualización continuas, tales como parches, para los cuales es necesaria una rápida evaluación o nueva certificación a fin de evitar impactos perjudiciales en la seguridad general de ese producto o servicio.*** |

Or. en

**Enmienda 340**
**Arndt Kohn, Sergio Gutiérrez Prieto, Pina Picierno, Christel Schaldemose**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra h bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***h bis) los casos específicos de nueva certificación de un producto y servicio de TIC se definirán en el régimen de certificación correspondiente. La seguridad y las actualizaciones de características con referencia a cualquier medida de seguridad deberán seguir un proceso de evaluación y, en caso necesario, de nueva certificación;*** |

Or. en

**Enmienda 341**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra i**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| ***i) normas relativas a las consecuencias de la no conformidad de los productos y servicios de TIC certificados con los requisitos de certificación;*** | ***suprimida*** |

Or. en

**Enmienda 342**
**Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra i**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| i) normas relativas a las consecuencias de la no conformidad de los productos y servicios de TIC certificados con los requisitos de certificación; | i) normas relativas a las consecuencias de la no conformidad de los productos y servicios ***de hardware y software*** de TIC certificados con los requisitos de certificación***, incluida la información general sobre las sanciones que se impondrán según lo establecido en el artículo 54 del presente Reglamento***; |

Or. en

**Enmienda 343**
**Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra j**

| *Texto de la Comisión* | *Enmienda* |
|---|---|

| | |
|---|---|
| j) normas sobre cómo deben notificarse y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios de TIC; | j) ***el requisito de que un proveedor de servicios o comerciante de productos de hardware y software de TIC haya establecido procedimientos y*** normas sobre cómo deben notificarse y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios ***de hardware y software*** de TIC; |

Or. en

*Justificación*

*Esto incluye una completa cadena de comunicación entre cliente, proveedor y fabricante para que los clientes finales puedan comunicar vulnerabilidades de ciberseguridad no detectadas al proveedor y al fabricante a fin de que se emitan parches o correcciones para abordarlas.*

**Enmienda 344**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra j**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| j) normas ***sobre cómo deben notificarse y tramitarse*** las vulnerabilidades ***de ciberseguridad previamente no detectadas*** en productos y servicios de TIC***;*** | j) normas ***que requieran que*** las vulnerabilidades en productos y servicios de TIC ***que no se conozcan públicamente se notifiquen rápidamente por parte de las autoridades adecuadas a los proveedores y fabricantes pertinentes mediante el uso de un proceso coordinado de divulgación de vulnerabilidades.*** |

Or. en

*Justificación*

*Esta tarea se ejecutará de conformidad con las directrices y las recomendaciones indicadas en las normas internacionales ISO/IEC 29147:2014 e ISO/IEC 30111.*

**Enmienda 345**
**Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra j**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| j) normas ***sobre cómo deben notificarse y tramitarse*** las vulnerabilidades ***de ciberseguridad previamente no detectadas*** en productos y servicios de TIC; | j) normas ***que requieran que*** las vulnerabilidades en productos y servicios de TIC ***que no se conozcan públicamente se notifiquen rápidamente por parte de las autoridades adecuadas a los proveedores y fabricantes pertinentes mediante el uso de un proceso coordinado de divulgación de vulnerabilidades***; |

Or. en

**Enmienda 346**
**Jiří Pospíšil**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra j**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| j) normas sobre cómo deben notificarse y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios de TIC; | j) normas sobre cómo deben notificarse y tramitarse las vulnerabilidades ***o lagunas*** de ciberseguridad previamente no detectadas en productos y servicios de TIC; |

Or. cs

**Enmienda 347**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra j**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| j) normas sobre cómo deben ***notificarse y*** tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios de TIC; | j) normas sobre cómo deben tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios de TIC; |

Or. en

**Enmienda 348**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra k**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| k) normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad; | k) ***en relación con la opción de certificación del régimen por parte de terceros mencionada en el artículo 47 bis, apartado 2, letra b),*** normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad; |

Or. en

**Enmienda 349**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra l**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos ***y*** servicios de TIC; | l) identificación de los regímenes nacionales ***o internacionales*** de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos***,*** servicios***, procesos, requisitos de seguridad y criterios y métodos de evaluación*** de ***las*** TIC; |

Or. en

**Enmienda 350**
**Roberta Metsola, Eva Maydell, Lara Comi**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra l**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC; | l) identificación de los regímenes nacionales de certificación de la ciberseguridad ***o de los métodos dirigidos por la industria*** que cubren el mismo tipo o categoría de productos y servicios ***de hardware y software*** de TIC; |

Or. en

**Enmienda 351**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra l**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo ***o*** categoría de productos y servicios de TIC; | l) identificación de los regímenes nacionales de certificación ***o autoevaluación*** de la ciberseguridad que cubren el mismo tipo ***de*** categoría de productos y servicios de TIC; ***y*** |

Or. en

**Enmienda 352**
**Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra l**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC; | l) identificación de los regímenes nacionales ***o internacionales*** de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC; |

Or. fr

**Enmienda 353**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra l bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***l bis) identificación de las certificaciones y los acuerdos de reconocimiento mutuo internacionales existentes;*** |

Or. en

**Enmienda 354**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) mecanismo de gobernanza para actualizar, modificar y coordinar determinados regímenes de certificación, en particular, especificación detallada sobre cómo debe modificarse un régimen de certificación a la luz de las amenazas adicionales para la seguridad, una vez que se conozcan;*** |

Or. en

**Enmienda 355**
**Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) normas relativas a la forma y el momento en que los Estados miembros deben informarse recíprocamente cuando*** |

***adquieren conocimiento de una vulnerabilidad que no se conozca públicamente en un producto o servicio de TIC certificado con arreglo a este régimen de certificación;***

Or. en

**Enmienda 356**
**Dennis de Jong**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) un mecanismo y herramientas para gestionar de forma eficiente el lanzamiento de versiones menores o actualizaciones de seguridad (por ejemplo, en relación con los parches);*** |

Or. en

*Justificación*

*Se necesita un mecanismo para corregir las actualizaciones de seguridad menores durante la vida útil del certificado con el fin de evitar un proceso largo y costoso de nueva certificación cada vez que se necesite una corrección o actualización. Este mecanismo es necesario para mantener el elevado ritmo de desarrollo y solucionar rápidamente los problemas de seguridad conocidos. Además, ya es una práctica común con otros certificados interesantes.*

**Enmienda 357**
**Philippe Juvin**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) el plazo máximo de validez de los certificados;*** |

Or. fr

**Enmienda 358**
**Anneleen Van Bossuyt, Daniel Dalton**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) el período de validez de los certificados emitidos.*** |

Or. en

**Enmienda 359**
**Roberta Metsola, Eva Maydell, Lara Comi**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m bis (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m bis) el período de validez del certificado*** |

Or. en

**Enmienda 360**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m ter (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m ter) pruebas de resistencia y resiliencia para los niveles de garantía «extremadamente seguro» y «sustancialmente seguro»;*** |

Or. en

**Enmienda 361**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 – letra m quater (nueva)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***m quater) cuando sea necesario, procedimientos de autodeclaración aplicables para el nivel de garantía «funcionalmente seguro»;*** |

Or. en

**Enmienda 362**
**Lambert van Nistelrooij**

**Propuesta de Reglamento**
**Artículo 47 – apartado 1 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***1 bis. Un mecanismo y herramientas para gestionar de forma eficiente el lanzamiento de versiones menores o actualizaciones de seguridad (por ejemplo, en relación con los parches).*** |

Or. en

*Justificación*

*Se necesita un mecanismo para corregir las actualizaciones de seguridad menores durante la vida útil del certificado con el fin de evitar un proceso largo y costoso de nueva certificación cada vez que se necesite una corrección o actualización. Este mecanismo es necesario para mantener el elevado ritmo de desarrollo y solucionar rápidamente los problemas de seguridad conocidos. Además, ya es una práctica común con otros certificados interesantes.*

**Enmienda 363**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 2**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 2. Los requisitos del régimen | 2. Los requisitos del régimen |

| | |
|---|---|
| especificados no podrán contravenir ningún requisito legal aplicable***, en particular los*** que ***emanen*** de la legislación armonizada de la Unión. | especificados no podrán contravenir ningún requisito legal aplicable que ***emane*** de la legislación armonizada de la Unión. |

Or. en

**Enmienda 364**
**Dita Charanzová, Morten Løkkegaard**

**Propuesta de Reglamento**
**Artículo 47 – apartado 3**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| 3. Cuando un acto específico de la Unión así lo prevea, podrá utilizarse la certificación en virtud de un régimen europeo de certificación de la ciberseguridad para demostrar la presunción de conformidad con los requisitos de dicho acto. | 3. Cuando un acto específico de la Unión así lo prevea, podrá utilizarse la certificación en virtud de un régimen europeo de certificación de la ciberseguridad ***como medio alternativo*** para demostrar la presunción de conformidad con los requisitos de dicho acto. |

Or. en

**Enmienda 365**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 – apartado 4 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***4 bis. Los regímenes creados con arreglo al presente Reglamento no requerirán notificación de cambios, modificaciones de certificaciones o nueva certificación, a menos que tales cambios tengan un efecto negativo sustancial en la seguridad de los productos y servicios de TIC. Esto incluye:*** |
| | ***a) una reducción en el ámbito de aplicación de un certificado;*** |

***b) mejoras de las prioridades mencionadas en el artículo 45;***

***c) actualizaciones de software, según lo mencionado en el artículo 45, letra c); y***

***d) cualquier otra medida destinada a abordar vulnerabilidades de ciberseguridad no detectadas anteriormente según lo indicado en el artículo 45, letra c).***

Or. en

**Enmienda 366**
**Antonio López-Istúriz White**

**Propuesta de Reglamento**
**Artículo 47 bis (nuevo)**

| *Texto de la Comisión* | *Enmienda* |
|---|---|
| | ***Artículo 47 bis*** |
| | ***Primera evaluación o evaluación de terceros*** |
| | ***1. Un régimen de ciberseguridad europeo ofrecerá opciones tanto para la autoevaluación como para la certificación de terceros, tal y como se describe en el apartado 2, letras a) y b) respectivamente.*** |
| | ***2. El fabricante o proveedor de productos y servicios de TIC podrá decidir libremente si la evaluación y la certificación de dichos productos o servicios en el marco de un régimen europeo de ciberseguridad la lleva a cabo:*** |
| | ***a) el propio fabricante o proveedor («autodeclaración») o*** |
| | ***b) un organismo de evaluación de la conformidad mencionado en el artículo 51 («certificación de terceros»).*** |

Or. en

*Justificación*

*Esta enmienda complementa la enmienda anterior al artículo 47 y garantiza que los futuros regímenes europeos de ciberseguridad ofrezcan opciones tanto para la autoevaluación como para la certificación de terceros. Corresponderá al fabricante del producto y servicio de TIC decidir si la evaluación debe realizarse mediante autoevaluación o por parte de terceros. Esto refleja el proceso actual ampliamente utilizado en determinados sectores industriales.*