



**A8-0084/2019**

22.2.2019

**\*\*\*I**

## **INFORME**

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación  
(COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

Comisión de Industria, Investigación y Energía

Ponente: Julia Reda

### ***Explicación de los signos utilizados***

- \* Procedimiento de consulta
- \*\*\* Procedimiento de aprobación
- \*\*\*I Procedimiento legislativo ordinario (primera lectura)
- \*\*\*II Procedimiento legislativo ordinario (segunda lectura)
- \*\*\*III Procedimiento legislativo ordinario (tercera lectura)

(El procedimiento indicado se sustenta en la base jurídica propuesta en el proyecto de acto).

### ***Enmiendas a un proyecto de acto***

#### **Enmiendas del Parlamento presentadas en dos columnas**

Las supresiones se señalan en ***cursiva y negrita*** en la columna izquierda. Las sustituciones se señalan en ***cursiva y negrita*** en ambas columnas. El texto nuevo se señala en ***cursiva y negrita*** en la columna derecha.

En las primeras dos líneas del encabezamiento de cada enmienda se indica el pasaje del proyecto de acto examinado que es objeto de la enmienda. Si una enmienda se refiere a un acto existente que se quiere modificar con el proyecto de acto, su encabezamiento contiene además una tercera y cuarta líneas en las que se indican, respectivamente, el acto existente y la disposición de que se trate.

#### **Enmiendas del Parlamento en forma de texto consolidado**

Las partes de texto nuevas se indican en ***cursiva y negrita***. Las partes de texto suprimidas se indican mediante el símbolo ¶ o se tachan. Las sustituciones se indican señalando el texto nuevo en ***cursiva y negrita*** y suprimiendo o tachando el texto sustituido.

Como excepción, no se marcan las modificaciones de carácter estrictamente técnico introducidas por los servicios para la elaboración del texto final.

## ÍNDICE

	<b>Página</b>
PROYECTO DE RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO .....	5
EXPOSICIÓN DE MOTIVOS .....	82
ANEXO: LISTA DE LAS ORGANIZACIONES O PERSONAS QUE HAN COLABORADO CON LA PONENTE.....	85
OPINIÓN DE LA COMISIÓN DE MERCADO INTERIOR Y PROTECCIÓN DEL CONSUMIDOR.....	86
PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EL FONDO.....	135
VOTACIÓN FINAL NOMINAL EN LA COMISIÓN COMPETENTE PARA EL FONDO .....	136



## PROYECTO DE RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

(Procedimiento legislativo ordinario: primera lectura)

*El Parlamento Europeo,*

- Vista la propuesta de la Comisión al Parlamento Europeo y al Consejo (COM(2018)0630),
  - Vistos el artículo 294, apartado 2, el artículo 173, apartado 3, y el párrafo primero del artículo 188 del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C8-0404/2018),
  - Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,
  - Visto el dictamen del Comité Económico y Social Europeo de 23 de enero de 2019<sup>1</sup>,
  - Visto el artículo 59 de su Reglamento interno,
  - Vistos el informe de la Comisión de Industria, Investigación y Energía y la opinión de la Comisión de Mercado Interior y Protección del Consumidor (A8-0084/2019),
1. Aprueba la Posición en primera lectura que figura a continuación;
  2. Pide a la Comisión que le consulte de nuevo si sustituye su propuesta, la modifica sustancialmente o se propone modificarla sustancialmente;
  3. Encarga a su presidente que transmita la Posición del Parlamento al Consejo y a la Comisión, así como a los Parlamentos nacionales.

### Enmienda 1

#### Propuesta de Reglamento

##### Considerando 1

*Texto de la Comisión*

(1) *A medida que* nuestra vida cotidiana y la economía se **vuelven** más dependientes de las tecnologías digitales, los ciudadanos están cada vez más expuestos a incidentes cibernéticos graves.

*Enmienda*

(1) **Más del 80 % de la población de la Unión está conectada a internet**, y nuestra vida cotidiana y la economía se **están volviendo** más dependientes de las tecnologías digitales, **al tiempo que** los

---

<sup>1</sup>Pendiente de publicación en el Diario Oficial.

La seguridad futura depende, entre otras cosas, de la mejora de la capacidad tecnológica e industrial para proteger a la Unión frente a las ciberamenazas, ya que tanto la infraestructura *civil* como las capacidades *militares* dependen de unos sistemas digitales seguros.

ciudadanos están cada vez más expuestos a incidentes cibernéticos graves. La seguridad futura depende, entre otras cosas, ***de la contribución a la resiliencia general*** y de la mejora de la capacidad tecnológica e industrial para proteger a la Unión frente a las ciberamenazas, ***en constante evolución***, ya que tanto la infraestructura como las capacidades ***de seguridad*** dependen de unos sistemas digitales seguros. ***Esto puede lograrse con la sensibilización con respecto a las amenazas para la ciberseguridad, mediante el desarrollo de competencias, capacidades y facultades en toda la Unión, teniendo plenamente en cuenta la interacción entre las infraestructuras de equipos y programas informáticos, las redes, los productos y los procesos, y las implicaciones y preocupaciones sociales y éticas.***

## Enmienda 2

### Propuesta de Reglamento Considerando 1 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

***(1 bis) La ciberdelincuencia representa una amenaza cada vez mayor para la Unión, sus ciudadanos y su economía. En 2017, el 80 % de las empresas europeas experimentó al menos un ciberincidente. El ataque Wannacry de mayo de 2017 afectó a más de 150 países y 230 000 sistemas informáticos y tuvo un impacto significativo en infraestructuras fundamentales como hospitales. Esto pone de manifiesto la necesidad de aplicar los niveles más elevados en materia de ciberseguridad y de buscar unas soluciones holísticas en este ámbito, que abarquen a las personas, los productos, los procesos y la tecnología en la Unión, así como la necesidad de un liderazgo europeo en la materia y de una autonomía***

*digital.*

### Enmienda 3

#### Propuesta de Reglamento Considerando 4

##### *Texto de la Comisión*

(4) En la Cumbre Digital de Tallin, celebrada en septiembre de 2017, los jefes de Estado y de Gobierno pidieron que la Unión se convirtiera en «un líder mundial en ciberseguridad para 2025, a fin de garantizar la confianza, la seguridad y la protección de nuestros ciudadanos, consumidores y empresas en línea y permitir una Internet libre, más segura y legal».

##### *Enmienda*

(4) En la Cumbre Digital de Tallin, celebrada en septiembre de 2017, los jefes de Estado y de Gobierno pidieron que la Unión se convirtiera en «un líder mundial en ciberseguridad para 2025, a fin de garantizar la confianza, la seguridad y la protección de nuestros ciudadanos, consumidores y empresas en línea y permitir una Internet libre, más segura y legal», **y declararon su intención de hacer un mayor uso de soluciones y estándares de código abierto a la hora de crear o renovar sistemas y soluciones TIC (también para evitar la dependencia de los proveedores), incluidos los desarrollados o promovidos por programas de la Unión en materia de interoperabilidad y normalización, como ISA<sup>2</sup>.**

### Enmienda 4

#### Propuesta de Reglamento Considerando 4 bis (nuevo)

##### *Texto de la Comisión*

##### *Enmienda*

**(4 bis) El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (en lo sucesivo, «el Centro de Competencia») debe contribuir a aumentar la resiliencia y fiabilidad de la infraestructura de las redes y los sistemas de información, incluidas internet y otras infraestructuras fundamentales para el funcionamiento de la sociedad, como los sistemas de transportes, los sistemas sanitarios y los sistemas bancarios.**

## Enmienda 5

### Propuesta de Reglamento Considerando 4 ter (nuevo)

*Texto de la Comisión*

*Enmienda*

**(4 ter) El Centro de Competencia y sus acciones deben tener en cuenta la aplicación del Reglamento (UE) 2019/XXX [refundición del Reglamento (CE) n.º 428/2009 propuesta por el documento COM(2016) 616]<sup>1bis</sup>.**

---

<sup>1 bis</sup> **Reglamento (UE) 2019/... del Parlamento Europeo y del Consejo, de ..., por el que se establece un régimen de la Unión de control de las exportaciones, la transferencia, el corretaje, la asistencia técnica y el tránsito de productos de doble uso (DO L [...] de [...], p. [...]).**

## Enmienda 6

### Propuesta de Reglamento Considerando 5

*Texto de la Comisión*

*Enmienda*

(5) Una perturbación grave de la red y los sistemas de información puede afectar a los distintos Estados miembros y a la Unión en su conjunto. Por consiguiente, **la** seguridad de las redes y sistemas de información es fundamental para **el correcto funcionamiento del mercado interior**. Actualmente, la Unión depende de proveedores de ciberseguridad no europeos. Sin embargo, es de interés estratégico para la Unión garantizar que se conservan y desarrollan las capacidades tecnológicas esenciales en materia de ciberseguridad para garantizar la **seguridad de su mercado único digital, y en particular para proteger** las redes y los sistemas de información fundamentales y

(5) Una perturbación grave de la red y los sistemas de información puede afectar a los distintos Estados miembros y a la Unión en su conjunto. Por consiguiente, **el máximo nivel de** seguridad de las redes y sistemas de información **en toda la Unión** es fundamental **tanto para la sociedad como para la economía**. Actualmente, la Unión depende de proveedores de ciberseguridad no europeos. Sin embargo, es de interés estratégico para la Unión garantizar que se conservan y desarrollan las capacidades **y competencias** tecnológicas esenciales en materia de ciberseguridad para garantizar la **protección de los datos y de** las redes y los sistemas de información fundamentales **de**



prestar servicios clave de ciberseguridad.

*las empresas y los ciudadanos europeos, incluidas las infraestructuras fundamentales para el funcionamiento de la sociedad, como los sistemas de transportes, los sistemas sanitarios y los sistemas bancarios, y del mercado único digital, y prestar servicios clave de ciberseguridad.*

## Enmienda 7

### Propuesta de Reglamento Considerando 6

#### *Texto de la Comisión*

(6) La Unión dispone de un amplio arsenal de conocimientos especializados y experiencia en investigación, tecnología y desarrollo industrial en el ámbito de la ciberseguridad, pero los esfuerzos de las comunidades industrial e investigadora están fragmentados, sin coordinación ni una misión común, lo que dificulta la competitividad en este ámbito. Es preciso poner en común estos esfuerzos y conocimientos especializados, conectarlos en red y usarlos de manera eficiente para reforzar y complementar las capacidades investigadoras, tecnológicas e industriales existentes a escala de la Unión y nacional.

#### *Enmienda*

(6) La Unión dispone de un amplio arsenal de conocimientos especializados y experiencia en investigación, tecnología y desarrollo industrial en el ámbito de la ciberseguridad, pero los esfuerzos de las comunidades industrial e investigadora están fragmentados, sin coordinación ni una misión común, lo que dificulta la competitividad **y la protección efectiva de los datos, redes y sistemas fundamentales** en este ámbito. Es preciso poner en común estos esfuerzos y conocimientos especializados, conectarlos en red y usarlos de manera eficiente para reforzar y complementar las capacidades investigadoras, tecnológicas, profesionales e industriales, **así como las competencias** existentes a escala de la Unión y nacional. ***Si bien el sector de las tecnologías de la información y la comunicación (TIC) se enfrenta a importantes retos, como satisfacer la demanda de trabajadores cualificados, puede beneficiarse de representar la diversidad del conjunto de la sociedad y alcanzar una representación equilibrada en lo que respecta a géneros, diversidad étnica y no discriminación de las personas con discapacidad, al igual que de facilitar el acceso a conocimientos y formación a futuros expertos en ciberseguridad, incluida su formación en contextos no formales, por ejemplo en proyectos de programas informáticos***

*libres y de código abierto, proyectos de tecnología cívica, empresas emergentes y microempresas.*

## **Enmienda 8**

### **Propuesta de Reglamento Considerando 6 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(6 bis) Las pequeñas y medianas empresas (pymes) son unos agentes fundamentales para el sector europeo de la ciberseguridad que pueden ofrecer soluciones punteras gracias a su agilidad. Sin embargo, las pymes no especializadas en ciberseguridad también tienden a ser más vulnerables a los ciberincidentes debido a los requisitos de altos niveles de inversión y conocimientos a la hora de aplicar unas soluciones efectivas en materia de ciberseguridad. Por consiguiente, es preciso que el Centro de Competencia y la red de competencias en ciberseguridad presten un apoyo especial a las pymes facilitando su acceso a los conocimientos y la formación, para que puedan protegerse lo suficiente y para que las pymes activas en el ámbito de la ciberseguridad contribuyan al liderazgo europeo en este ámbito.*

## **Enmienda 9**

### **Propuesta de Reglamento Considerando 6 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(6 ter) Los conocimientos especializados no se encuentran únicamente en los contextos industriales y de investigación. Los proyectos no comerciales y precomerciales, denominados «proyectos de tecnología cívica» utilizan estándares de código abierto, datos abiertos y programas informáticos libres y de código*

*abierto en interés de la sociedad y el bien público. Estos proyectos contribuyen a la resiliencia, la sensibilización y el desarrollo de competencias en cuestiones de ciberseguridad, y desempeñan un papel muy importante en la creación de capacidades para la industria y la investigación en este ámbito.*

## Enmienda 10

### Propuesta de Reglamento Considerando 6 quater (nuevo)

*Texto de la Comisión*

*Enmienda*

*(6 quater) En el contexto del presente Reglamento, los términos «partes interesadas» se refieren, entre otras partes, a la industria, las entidades públicas y otras entidades que se ocupen de cuestiones operativas y técnicas en el ámbito de la ciberseguridad, así como a la sociedad civil, en particular los sindicatos, las asociaciones de consumidores, la comunidad de programas informáticos libres y de código abierto, y la comunidad académica e investigadora.*

## Enmienda 11

### Propuesta de Reglamento Considerando 8

*Texto de la Comisión*

*Enmienda*

(8) El Centro de Competencia ha de ser el principal instrumento de la Unión para poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad y ejecutar los proyectos e iniciativas pertinentes junto con la red de competencias en ciberseguridad. Debe prestar apoyo financiero en relación con la ciberseguridad a través de los programas Horizonte Europa y Europa Digital, y estar abierto al Fondo Europeo de Desarrollo

(8) El Centro de Competencia ha de ser el principal instrumento de la Unión para poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad y ejecutar los proyectos e iniciativas pertinentes junto con la red de competencias en ciberseguridad. Debe prestar apoyo financiero en relación con la ciberseguridad a través de los programas Horizonte Europa y Europa Digital, **así como del Fondo Europeo de Defensa por**

Regional y a otros programas cuando proceda. Se espera que este enfoque contribuya a crear sinergias, coordinar el apoyo financiero relacionado con la **investigación**, la innovación, la tecnología y el desarrollo industrial en materia de ciberseguridad, y evitar la duplicación.

**lo que respecta a las acciones y los costes administrativos relativos a la defensa**, y estar abierto al Fondo Europeo de Desarrollo Regional y a otros programas cuando proceda. Se espera que este enfoque contribuya a crear sinergias, coordinar el apoyo financiero relacionado con **iniciativas de la Unión en el ámbito de la I+D**, la innovación, la tecnología y el desarrollo industrial en materia de ciberseguridad, y evitar la duplicación.

## Enmienda 12

### Propuesta de Reglamento Considerando 8 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

**(8 bis) La «seguridad mediante el diseño», principio establecido en la Comunicación conjunta de la Comisión, de 13 de septiembre de 2017, titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», incluye métodos de vanguardia para aumentar la seguridad, en todas las etapas del ciclo de vida de un producto o servicio, empezando por métodos seguros de diseño y desarrollo, reduciendo la superficie de ataque e incorporando pruebas de seguridad y auditorías de seguridad adecuadas. Por lo que respecta a la duración de la utilización y del mantenimiento, los productores o proveedores deben poner a disposición actualizaciones que subsanen las nuevas vulnerabilidades o amenazas sin demora durante la vida útil estimada de un producto y al término de esta. Esto también puede lograrse permitiendo a terceros crear y facilitar tales actualizaciones. La puesta a disposición de actualizaciones es especialmente necesaria en el caso de infraestructuras, productos y procesos de uso común.**

## Enmienda 13

### Propuesta de Reglamento Considerando 8 ter (nuevo)

*Texto de la Comisión*

*Enmienda*

***(8 ter) Ante el alcance de los desafíos en materia de ciberseguridad y las inversiones en capacidades y competencias en el ámbito de la ciberseguridad en otras partes del mundo, la Unión y sus Estados miembros deben reforzar su apoyo financiero a la investigación, el desarrollo y la implantación en este ámbito. Con objeto de lograr economías de escala y de conseguir un nivel de protección comparable en toda la Unión, los Estados miembros deben concentrar sus esfuerzos en un marco europeo invirtiendo a través del mecanismo del Centro de Competencia, cuando proceda.***

## Enmienda 14

### Propuesta de Reglamento Considerando 8 quater (nuevo)

*Texto de la Comisión*

*Enmienda*

***(8 quater) A fin de fomentar la competitividad europea y los niveles más altos en materia de ciberseguridad a escala internacional, el Centro de Competencia y la Comunidad deben propiciar los intercambios relativos a productos, procesos, normas y normas técnicas de ciberseguridad con la comunidad internacional. Las normas técnicas incluyen la creación de ejecuciones de referencia, publicadas en licencias abiertas y libres. El diseño seguro, en particular cuando se trata de ejecuciones de referencia, es fundamental para la fiabilidad y la resiliencia generales de las infraestructuras de red y sistemas de información de uso común, como internet y las infraestructuras***

*fundamentales.*

## Enmienda 15

### Propuesta de Reglamento Considerando 9

#### *Texto de la Comisión*

(9) Teniendo en cuenta que los objetivos de la presente iniciativa pueden alcanzarse mejor si **participan** todos los Estados miembros o el mayor número posible de Estados miembros, y como incentivo para su participación, solo aquellos que contribuyan financieramente a los costes administrativos y de funcionamiento del Centro de Competencia deben tener derecho de voto.

#### *Enmienda*

(9) Teniendo en cuenta que los objetivos de la presente iniciativa pueden alcanzarse mejor si **contribuyen** todos los Estados miembros o el mayor número posible de Estados miembros, y como incentivo para su participación, solo aquellos que contribuyan financieramente a los costes administrativos y de funcionamiento del Centro de Competencia deben tener derecho de voto.

## Enmienda 16

### Propuesta de Reglamento Considerando 12

#### *Texto de la Comisión*

(12) Los Estados miembros deben seleccionar los centros nacionales de coordinación. Además de la capacidad administrativa necesaria, los centros han de poseer o tener acceso directo a conocimientos tecnológicos especializados en materia de ciberseguridad, especialmente en ámbitos como la criptografía, los servicios de seguridad de TIC, la detección de intrusiones, la seguridad de los sistemas, la seguridad de las redes, la seguridad de los programas informáticos y las aplicaciones, o los aspectos humanos y sociales de la seguridad y la privacidad. También se requiere que tengan la capacidad de comprometerse y coordinarse eficazmente con la industria, el sector público, incluidas las autoridades designadas con arreglo a la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo<sup>23</sup>, y la comunidad

#### *Enmienda*

(12) Los Estados miembros deben seleccionar los centros nacionales de coordinación. Además de la capacidad administrativa necesaria, los centros han de poseer o tener acceso directo a conocimientos tecnológicos especializados en materia de ciberseguridad, especialmente en ámbitos como la criptografía, los servicios de seguridad de TIC, la detección de intrusiones, la seguridad de los sistemas, la seguridad de las redes, la seguridad de los programas informáticos y las aplicaciones, o los aspectos humanos, **éticos**, sociales y **medioambientales** de la seguridad y la privacidad. También se requiere que tengan la capacidad de comprometerse y coordinarse eficazmente con la industria, el sector público, incluidas las autoridades designadas con arreglo a la Directiva (UE) 2016/1148 del Parlamento Europeo y del

investigadora.

Consejo<sup>23</sup>, y la comunidad investigadora, **a fin de establecer un diálogo permanente público-privado sobre la ciberseguridad. Por otra parte, debe concienciarse al público, a través de los medios de comunicación adecuados, de la importancia de la ciberseguridad.**

---

<sup>23</sup> 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. 1).

---

<sup>23</sup> 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. 1).

## Enmienda 17

### Propuesta de Reglamento Considerando 14

#### *Texto de la Comisión*

(14) Las tecnologías emergentes, como la inteligencia artificial, el internet de las cosas, la informática de alto rendimiento (HPC) y la informática cuántica **o la cadena de bloques**, y conceptos como las identidades digitales seguras plantean nuevos retos para la ciberseguridad al mismo tiempo que ofrecen **soluciones**. A fin de determinar y validar la solidez de los sistemas TIC existentes o futuros, será necesario someter **las soluciones** de seguridad a pruebas frente a los ataques que se ejecutan en máquinas HPC y cuánticas. El Centro de Competencia, la Red y la Comunidad de Competencias en Ciberseguridad deben ayudar a impulsar y difundir **las últimas soluciones** en materia de ciberseguridad. **Paralelamente**, el Centro de Competencia y la Red han de estar al servicio de los desarrolladores y operadores de sectores fundamentales como el transporte, la energía, la salud, el sector financiero, el sector público, las telecomunicaciones, la industria manufacturera, la defensa o el espacio, a

#### *Enmienda*

(14) Las tecnologías emergentes, como la inteligencia artificial, el internet de las cosas, la informática de alto rendimiento (HPC) y la informática cuántica, **así como** conceptos como las identidades digitales seguras plantean nuevos retos para la ciberseguridad al mismo tiempo que ofrecen **productos y procesos**. A fin de determinar y validar la solidez de los sistemas TIC existentes o futuros, será necesario someter **los productos y procesos** de seguridad a pruebas frente a los ataques que se ejecutan en máquinas HPC y cuánticas. El Centro de Competencia, la Red, **los centros europeos de innovación digital** y la Comunidad de Competencias en Ciberseguridad deben ayudar a impulsar y difundir **los últimos productos y procesos** en materia de ciberseguridad, **incluido el doble uso, y en particular los que ayuden a las organizaciones a desarrollar constantemente sus capacidades, su resiliencia y una gobernanza adecuada**. El Centro de Competencia y la Red **deben estimular**

fin de ayudarles a resolver sus problemas relacionados con la ciberseguridad.

*todo el ciclo de innovación y contribuir a superar la fase de bajo rendimiento de la innovación en las tecnologías y los servicios en materia de ciberseguridad. Paralelamente, el Centro de Competencia, la Red y la Comunidad han de estar al servicio de los desarrolladores y operadores de sectores fundamentales como el transporte, la energía, la salud, el sector financiero, el sector público, las telecomunicaciones, la industria manufacturera, la defensa o el espacio, a fin de ayudarles a resolver sus problemas relacionados con la ciberseguridad, e investigar las distintas motivaciones de los ataques contra la integridad de las redes y los sistemas de información, como delincuencia, espionaje industrial, difamación y desinformación.*

## **Enmienda 18**

### **Propuesta de Reglamento Considerando 14 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(14 bis) Debido a la rapidez con que cambian las ciberamenazas y la ciberseguridad, la Unión debe poder estar en condiciones de adaptarse rápida y continuamente a la evolución más reciente en este ámbito. Por esta razón, el Centro de Competencia, la red de competencias en ciberseguridad y la Comunidad deben ser lo bastante flexibles como para garantizar la capacidad de respuesta requerida. Deben favorecer soluciones que ayuden a las entidades a poder desarrollar sus capacidades constantemente a fin de aumentar su resiliencia y la de la Unión.*

## **Enmienda 19**

### **Propuesta de Reglamento Considerando 14 ter (nuevo)**

PE631.940v02-00

16/136

RR\1177820ES.docx



*(14 ter) Los objetivos del Centro de Competencia deben ser establecer el liderazgo y los conocimientos especializados en ciberseguridad a escala europea, garantizando de este modo las normas de seguridad más elevadas en la Unión; garantizar la protección de los datos, de los sistemas de información, de las redes y de las infraestructuras fundamentales en la Unión; crear nuevos puestos de trabajo de calidad en este ámbito; evitar la fuga de cerebros, en este caso de expertos europeos en ciberseguridad, hacia terceros países; y conferir un valor añadido europeo a las medidas en materia de ciberseguridad que ya existen a escala nacional.*

## Enmienda 20

### Propuesta de Reglamento Considerando 15

(15) El Centro de Competencia debe tener varias funciones clave. En primer lugar, el Centro de Competencia debe facilitar y ayudar a coordinar la labor de la red europea de competencias en ciberseguridad y apoyar a la Comunidad de Competencias en Ciberseguridad. El Centro ha de impulsar el programa tecnológico de ciberseguridad y facilitar el acceso a los conocimientos especializados reunidos en la Red y en la Comunidad de Competencias en Ciberseguridad. En segundo lugar, es preciso que ejecute las partes pertinentes de los programas Europa Digital y Horizonte Europa mediante la concesión de subvenciones, normalmente tras una convocatoria de propuestas competitiva. En tercer lugar, el Centro de Competencia debe facilitar la inversión conjunta por la Unión, los Estados miembros y/o la industria.

(15) El Centro de Competencia debe tener varias funciones clave. En primer lugar, el Centro de Competencia debe facilitar y ayudar a coordinar la labor de la red europea de competencias en ciberseguridad y apoyar a la Comunidad de Competencias en Ciberseguridad. El Centro ha de impulsar el programa tecnológico de ciberseguridad **y poner en común, compartir** y facilitar el acceso a los conocimientos especializados reunidos en la Red y en la Comunidad de Competencias en Ciberseguridad, **así como a las infraestructuras de ciberseguridad**. En segundo lugar, es preciso que ejecute las partes pertinentes de los programas Europa Digital y Horizonte Europa mediante la concesión de subvenciones, normalmente tras una convocatoria de propuestas competitiva. En tercer lugar, el Centro de Competencia debe facilitar la

inversión conjunta por la Unión, los Estados miembros y/o la industria, **así como las posibilidades de formación conjunta y los programas de sensibilización, en consonancia con el programa Europa Digital, para que los ciudadanos y las empresas colmen el déficit de capacidades. Debe prestar especial atención a la preparación de las pymes en el ámbito de la ciberseguridad.**

## Enmienda 21

### Propuesta de Reglamento Considerando 16

#### *Texto de la Comisión*

(16) El Centro de Competencia ha de estimular y respaldar la cooperación y **la** coordinación de las actividades de la Comunidad de Competencias en Ciberseguridad, en la que participará un grupo amplio, abierto y diverso de agentes del ámbito de la tecnología de ciberseguridad. Dicha comunidad debe contar, en particular, con entidades de investigación, industrias de la oferta, industrias de la demanda y el sector público. Es preciso que la Comunidad de Competencias en Ciberseguridad contribuya a las actividades y al plan de trabajo del Centro de Competencia y que se beneficie asimismo de las actividades de desarrollo comunitario del Centro de Competencia y de la Red; sin embargo, no debe recibir un trato privilegiado en lo que respecta a las convocatorias de propuestas o licitaciones.

#### *Enmienda*

(16) El Centro de Competencia ha de estimular y respaldar la cooperación y coordinación **estratégica a largo plazo** de las actividades de la Comunidad de Competencias en Ciberseguridad, en la que participará un grupo amplio, abierto, **interdisciplinario** y diverso de agentes **europeos** del ámbito de la tecnología de ciberseguridad. Dicha comunidad debe contar, en particular, con entidades de investigación, **incluidas aquellas que se dedican a la ética en el ámbito de la ciberseguridad**, industrias de la oferta, industrias de la demanda, **incluidas las pymes**, y el sector público. Es preciso que la Comunidad de Competencias en Ciberseguridad contribuya a las actividades y al plan de trabajo del Centro de Competencia y que se beneficie asimismo de las actividades de desarrollo comunitario del Centro de Competencia y de la Red; sin embargo, no debe recibir un trato privilegiado en lo que respecta a las convocatorias de propuestas o licitaciones.

## Enmienda 22

### Propuesta de Reglamento Considerando 16 bis (nuevo)

**(16 bis) El Centro de Competencia debe prestar la ayuda adecuada a la ENISA en los cometidos que se le han asignado en virtud de la Directiva (UE) 2016/1148 («Directiva SRI») y el Reglamento (UE) 2019/XXX del Parlamento Europeo y del Consejo («Reglamento de Ciberseguridad»)<sup>1 bis</sup>. Por consiguiente, la ENISA debe aportar las contribuciones pertinentes al Centro de Competencia en su cometido de determinar las prioridades de financiación.**

---

<sup>1a</sup> **Reglamento (UE) 2019/... del Parlamento Europeo y del Consejo, de ..., relativo a la 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») (DO L [...] de [...], p. [...]) (2017/0225(COD)).**

## Enmienda 23

### Propuesta de Reglamento Considerando 17

Texto de la Comisión

Enmienda

(17) Para dar respuesta a las necesidades de las industrias de la demanda y de la oferta, la función del Centro de Competencia de proporcionar a las industrias conocimientos y asistencia técnica en materia de ciberseguridad ha de referirse tanto a los productos y servicios de TIC como a todos los demás productos y **soluciones** industriales y tecnológicos en los que deba integrarse la ciberseguridad.

(17) Para dar respuesta a las necesidades **del sector público** y de las industrias de la demanda y de la oferta, la función del Centro de Competencia de proporcionar **al sector público** y a las industrias conocimientos y asistencia técnica en materia de ciberseguridad ha de referirse tanto a los productos, **procesos** y servicios de TIC como a todos los demás productos y **procesos** industriales y tecnológicos en los que deba integrarse la ciberseguridad. **En particular, el Centro de Competencia debe facilitar la aplicación de soluciones dinámicas a escala de las empresas,**

*centradas en el desarrollo de las capacidades de las organizaciones en su conjunto, incluidas las personas, los procesos y la tecnología, a fin de proteger eficazmente a las organizaciones frente a unas ciberamenazas que cambian constantemente.*

## Enmienda 24

### Propuesta de Reglamento Considerando 17 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

*(17 bis) El Centro de Competencia debe contribuir a una amplia implantación de productos y soluciones de ciberseguridad de última generación, en particular de aquellos que gozan de reconocimiento internacional.*

## Enmienda 25

### Propuesta de Reglamento Considerando 18

*Texto de la Comisión*

*Enmienda*

(18) Mientras que el Centro de Competencia y la Red deben esforzarse por lograr sinergias entre los ámbitos civil y militar de la ciberseguridad, los proyectos financiados por el programa Horizonte Europa se ejecutarán de conformidad con el Reglamento XXX [Reglamento relativo a Horizonte Europa], que dispone que las actividades de investigación e innovación llevadas a cabo en el marco de Horizonte Europa se centrarán en las aplicaciones civiles.

(18) Mientras que el Centro de Competencia y la Red deben esforzarse por lograr sinergias **y la coordinación** entre los ámbitos civil y militar de la ciberseguridad, los proyectos financiados por el programa Horizonte Europa se ejecutarán de conformidad con el Reglamento XXX [Reglamento relativo a Horizonte Europa], que dispone que las actividades de investigación e innovación llevadas a cabo en el marco de Horizonte Europa se centrarán en las aplicaciones civiles.

## Enmienda 26

### Propuesta de Reglamento Considerando 19

*Texto de la Comisión*

(19) Con el objetivo de garantizar una colaboración estructurada y duradera, es conveniente que la relación entre el Centro de Competencia y los centros nacionales de coordinación se base en un acuerdo contractual.

*Enmienda*

(19) Con el objetivo de garantizar una colaboración estructurada y duradera, es conveniente que la relación entre el Centro de Competencia y los centros nacionales de coordinación se base en un acuerdo contractual ***que debe armonizarse a escala de la Unión.***

**Enmienda 27**

**Propuesta de Reglamento  
Considerando 20**

*Texto de la Comisión*

(20) Se deben establecer disposiciones adecuadas para garantizar la responsabilidad y la transparencia del Centro de Competencia.

*Enmienda*

(20) Se deben establecer disposiciones adecuadas para garantizar la responsabilidad y la transparencia del Centro de Competencia ***y de las empresas que reciban financiación.***

**Enmienda 28**

**Propuesta de Reglamento  
Considerando 20 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(20 bis) La ejecución de proyectos de implantación, en particular los relacionados con las infraestructuras y capacidades desplegadas a escala europea o en régimen de contratación conjunta, puede dividirse en distintas fases de ejecución, por ejemplo licitaciones separadas para la arquitectura del equipo informático y de los programas informáticos, su producción y su funcionamiento y mantenimiento, con la condición de que las empresas solo podrán participar en una de las fases cada una y con la exigencia de que los beneficiarios de una o varias de dichas fases satisfagan determinadas condiciones***

*en términos de propiedad o control europeos.*

*Justificación*

*Las licitaciones separadas para la arquitectura del equipo informático y de los programas informáticos, su producción y su funcionamiento y mantenimiento contribuirían en gran medida a la transparencia y la seguridad.*

**Enmienda 29**

**Propuesta de Reglamento  
Considerando 20 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

**(20 ter)** *Dado que la ENISA es la agencia europea especializada en ciberseguridad, el Centro de Competencia debe procurar maximizar las sinergias con ella, y el Consejo de Administración debe consultar a la ENISA, habida cuenta de su experiencia en este ámbito en todo lo relacionado con la ciberseguridad, especialmente en lo que respecta a los proyectos relacionados con la investigación.*

**Enmienda 30**

**Propuesta de Reglamento  
Considerando 20 quater (nuevo)**

*Texto de la Comisión*

*Enmienda*

**(20 quater)** *En el proceso de nombramiento del representante en el Consejo de Administración, el Parlamento Europeo debe incluir pormenores sobre el mandato, incluida la obligación de informar periódicamente al Parlamento Europeo o a las comisiones competentes.*

**Enmienda 31**

**Propuesta de Reglamento  
Considerando 21**

*Texto de la Comisión*

(21) Habida cuenta de sus respectivos conocimientos especializados en materia de ciberseguridad, procede que el Centro Común de Investigación de la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) desempeñen un papel activo en la Comunidad de Competencias en Ciberseguridad y en el Consejo Consultivo Industrial y Científico.

*Enmienda*

(21) Habida cuenta de sus respectivos conocimientos especializados en materia de ciberseguridad, **y con el fin de maximizar las sinergias**, procede que el Centro Común de Investigación de la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) desempeñen un papel activo en la Comunidad de Competencias en Ciberseguridad y en el Consejo Consultivo Industrial y Científico. **La ENISA debe seguir cumpliendo sus objetivos estratégicos, especialmente en el ámbito de la certificación de la ciberseguridad, tal como se establece en el Reglamento (UE) 2019/XXX [Reglamento de Ciberseguridad]<sup>1 bis</sup>, mientras que el Centro de Competencia debe actuar como órgano operativo en el ámbito de la ciberseguridad.**

---

<sup>1 bis</sup> **Reglamento (UE) 2019/... del Parlamento Europeo y del Consejo, de ..., relativo a la 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») (DO L [...] de [...], p. [...]) (2017/0225(COD)).**

**Enmienda 32**

**Propuesta de Reglamento  
Considerando 24**

*Texto de la Comisión*

(24) El Consejo de Administración del Centro de Competencia, integrado por los Estados miembros y la Comisión, debe definir la orientación general del funcionamiento del Centro de Competencia

*Enmienda*

(24) El Consejo de Administración del Centro de Competencia, integrado por los Estados miembros y la Comisión, debe definir la orientación general del funcionamiento del Centro de Competencia

y garantizar que desempeña su cometido de conformidad con el presente Reglamento. Es preciso que el Consejo de Administración esté dotado de las facultades necesarias para establecer el presupuesto, supervisar su ejecución, adoptar las correspondientes normas financieras, establecer procedimientos de trabajo transparentes para la toma de decisiones por el Centro de Competencia, adoptar el plan de trabajo y el plan estratégico plurianual del Centro de Competencia que reflejen las prioridades para lograr los objetivos y las tareas de dicho Centro, adoptar su reglamento interno, nombrar al director ejecutivo y acordar la prolongación del mandato del director ejecutivo o su cese.

y garantizar que desempeña su cometido de conformidad con el presente Reglamento. Es preciso que el Consejo de Administración esté dotado de las facultades necesarias para establecer el presupuesto, supervisar su ejecución, adoptar las correspondientes normas financieras, establecer procedimientos de trabajo transparentes para la toma de decisiones por el Centro de Competencia, adoptar el plan de trabajo y el plan estratégico plurianual del Centro de Competencia que reflejen las prioridades para lograr los objetivos y las tareas de dicho Centro, adoptar su reglamento interno, nombrar al director ejecutivo y acordar la prolongación del mandato del director ejecutivo o su cese. ***A fin de aprovechar las sinergias, la ENISA debe tener la condición de observador permanente en el Consejo de Administración y contribuir a la labor del Centro de Competencia, por ejemplo siendo consultada acerca del plan estratégico plurianual y sobre el plan de trabajo, así como sobre la lista de acciones seleccionadas para su financiación.***

### **Enmienda 33**

#### **Propuesta de Reglamento Considerando 24 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(24 bis) El Consejo de Administración debe tratar de promocionar el Centro de Competencia en todo el mundo, a fin de aumentar su atractivo y convertirlo en un organismo de categoría mundial por su excelencia en materia de ciberseguridad.***

### **Enmienda 34**

#### **Propuesta de Reglamento Considerando 25**



*Texto de la Comisión*

(25) Para que el Centro de Competencia funcione correcta y eficazmente, la Comisión y los Estados miembros han de garantizar que las personas que se nombren como miembros del Consejo de Administración disponen 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.

*Enmienda*

(25) Para que el Centro de Competencia funcione correcta y eficazmente, la Comisión y los Estados miembros han de garantizar que las personas que se nombren como miembros del Consejo de Administración disponen 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, **y deben aspirar a lograr el equilibrio de género.**

**Enmienda 35**

**Propuesta de Reglamento  
Considerando 25 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**(25 bis) El peso del voto de la Comisión en las decisiones del Consejo de Administración debe ser acorde con la contribución del presupuesto de la Unión al Centro de Competencia, con arreglo a la responsabilidad de la Comisión a la hora de garantizar una gestión adecuada del presupuesto de la Unión en interés de la Unión, tal como establecen los Tratados.**

**Enmienda 36**

**Propuesta de Reglamento  
Considerando 26**

*Texto de la Comisión*

*Enmienda*

(26) En aras del buen funcionamiento del Centro de Competencia, es preciso que su director ejecutivo sea nombrado

(26) En aras del buen funcionamiento del Centro de Competencia, es preciso que su director ejecutivo sea nombrado **de**

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.

*forma transparente* 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.

## Enmienda 37

### Propuesta de Reglamento Considerando 27

#### *Texto de la Comisión*

(27) El Centro de Competencia debe contar con un Consejo Consultivo Industrial y Científico 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 Consejo Consultivo Industrial y Científico ha de centrarse en las cuestiones que afecten a las partes interesadas y ponerlas en conocimiento del Consejo de Administración del Centro de Competencia. La composición del Consejo Consultivo Industrial y Científico y las funciones asignadas a este, como la de ser consultado respecto al plan de trabajo, deben garantizar una representación suficiente de las partes interesadas en la labor del Centro de Competencia.

#### *Enmienda*

(27) El Centro de Competencia debe contar con un Consejo Consultivo Industrial y Científico en calidad de organismo consultivo, a fin de garantizar un diálogo sistemático *y suficientemente transparente* con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes. ***También debe proporcionar asesoramiento independiente en materia de implantación y contratación pública al director ejecutivo y al Consejo de Administración.*** El Consejo Consultivo Industrial y Científico ha de centrarse en las cuestiones que afecten a las partes interesadas y ponerlas en conocimiento del Consejo de Administración del Centro de Competencia. La composición del Consejo Consultivo Industrial y Científico y las funciones asignadas a este, como la de ser consultado respecto al plan de trabajo, deben garantizar una representación suficiente de las partes interesadas en la labor del Centro de Competencia. ***Se debe asignar un mínimo de miembros a cada categoría de partes interesadas de la industria, prestando especial atención a la representación de las pymes.***

## Enmienda 38

### Propuesta de Reglamento

## Considerando 28

### *Texto de la Comisión*

(28) Es preciso que el Centro de Competencia, mediante su Consejo Consultivo Industrial y Científico, se **beneficie** de los conocimientos especializados y la amplia y pertinente representación de partes interesadas que se han logrado a través de la asociación público-privada contractual sobre ciberseguridad durante la ejecución de Horizonte 2020.

### *Enmienda*

(28) Es preciso que el Centro de Competencia **y sus actividades**, mediante su Consejo Consultivo Industrial y Científico, se **beneficien** de los conocimientos especializados y la amplia y pertinente representación de partes interesadas que se han logrado a través de la asociación público-privada contractual sobre ciberseguridad durante la ejecución de Horizonte 2020 **y los proyectos piloto en el contexto de Horizonte 2020 sobre la red de competencias en ciberseguridad. El Centro de Competencia y el Consejo Consultivo Industrial y Científico deben, en su caso, examinar la posibilidad de reproducir estructuras existentes, por ejemplo en forma de grupos de trabajo.**

## Enmienda 39

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

### *Texto de la Comisión*

### *Enmienda*

**(28 bis) El Centro de Competencia y sus órganos deben utilizar la experiencia y las contribuciones de iniciativas pasadas y en curso, como la asociación público-privada contractual sobre ciberseguridad, la Organización de Ciberseguridad Europea, y el proyecto piloto y la acción preparatoria sobre auditorías de programas informáticos libres y de código abierto.**

## Enmienda 40

### **Propuesta de Reglamento Considerando 29**

### *Texto de la Comisión*

### *Enmienda*

(29) El Centro de Competencia ha de contar con normas para la prevención y

(29) El Centro de Competencia ha de contar con normas para la prevención,

**gestión** de los conflictos de intereses. El Centro de Competencia debe aplicar, asimismo, las correspondientes disposiciones de la Unión relativas al acceso del público a los documentos, según se establece en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo<sup>24</sup>. El tratamiento de los datos personales por parte del Centro de Competencia se ajustará al Reglamento (UE) n.º XXX/2018 del Parlamento Europeo y del Consejo. El Centro de Competencia debe cumplir las disposiciones aplicables a las instituciones de la Unión, así como la legislación nacional en materia de tratamiento de la información, en particular la información delicada no clasificada y la información clasificada de la UE.

---

<sup>24</sup> Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

**detección y resolución** de los conflictos de intereses **por lo que se refiere a sus miembros, órganos y personal, al Consejo de Administración así como al Consejo Consultivo Industrial y Científico y a la Comunidad. Los Estados miembros deben garantizar la prevención, la detección y la resolución de los conflictos de intereses con respecto a los centros nacionales de coordinación.** El Centro de Competencia debe aplicar, asimismo, las correspondientes disposiciones de la Unión relativas al acceso del público a los documentos, según se establece en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo<sup>24</sup>. El tratamiento de los datos personales por parte del Centro de Competencia se ajustará al Reglamento (UE) n.º XXX/2018 del Parlamento Europeo y del Consejo. El Centro de Competencia debe cumplir las disposiciones aplicables a las instituciones de la Unión, así como la legislación nacional en materia de tratamiento de la información, en particular la información delicada no clasificada y la información clasificada de la UE.

---

<sup>24</sup> Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

## Enmienda 41

### Propuesta de Reglamento Considerando 31

#### *Texto de la Comisión*

(31) El Centro de Competencia debe funcionar de manera abierta y transparente, facilitando en el momento adecuado **toda la información pertinente** y promocionando sus actividades, en particular mediante actividades de

#### *Enmienda*

(31) El Centro de Competencia debe funcionar de manera abierta y transparente, facilitando **información de manera exhaustiva** y en el momento adecuado y promocionando sus actividades, en particular mediante actividades de

información y difusión destinadas al público en general. Debe hacerse público el reglamento interno de los órganos del Centro de Competencia.

información y difusión destinadas al público en general. ***Debe facilitar al público y a cualquier parte interesada una lista de los miembros de la Comunidad de Competencias en Ciberseguridad y hacer públicas las declaraciones de intereses que presenten de conformidad con el artículo 42.*** Debe hacerse público el reglamento interno de los órganos del Centro de Competencia.

## **Enmienda 42**

### **Propuesta de Reglamento Considerando 31 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(31 bis) Sería recomendable que tanto el Centro de Competencia como los centros nacionales de coordinación supervisarán las normas internacionales e hicieran un seguimiento de ellas en la medida de lo posible, a fin de promover la elaboración de buenas prácticas mundiales.***

## **Enmienda 43**

### **Propuesta de Reglamento Considerando 33 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(33 bis) Deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea, por lo que respecta a la definición de los elementos de los acuerdos contractuales entre el Centro de Competencia y los centros nacionales de coordinación, así como a la especificación de los criterios para la evaluación y acreditación de las entidades en cuanto miembros de la Comunidad de Competencias en Ciberseguridad. 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 de 13 de abril de 2016 sobre la mejora de la legislación<sup>1 bis</sup>. 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.*

---

<sup>1a</sup> DO L 123 de 12.5.2013, p. 1.

#### Enmienda 44

#### Propuesta de Reglamento Considerando 34

##### *Texto de la Comisión*

(34) **Dado que** los objetivos del presente Reglamento, a saber, mantener y desarrollar las capacidades tecnológicas e industriales de la Unión en materia de ciberseguridad, aumentar la competitividad de la industria de ciberseguridad de la Unión y convertir la ciberseguridad en una ventaja competitiva de otras industrias de la Unión, no pueden ser alcanzados de manera suficiente por los Estados miembros debido al hecho de que los recursos existentes son limitados y están dispersos, así como debido a la magnitud de las inversiones necesarias, sino que, a fin de evitar la duplicación innecesaria de los esfuerzos, ayudar a lograr una masa crítica de inversión y garantizar que la financiación pública se usa de forma óptima, **dichos objetivos** pueden alcanzarse mejor a escala de la Unión, **esta** puede adoptar medidas, de **conformidad** con el

##### *Enmienda*

(34) Los objetivos del presente Reglamento, a saber, **reforzar la competitividad y las capacidades de la Unión en materia de ciberseguridad, y reducir su dependencia digital mediante una mayor asimilación de productos, procesos y servicios de ciberseguridad desarrollados en la Unión**, mantener y desarrollar las capacidades tecnológicas e industriales de la Unión en materia de ciberseguridad, aumentar la competitividad de la industria de ciberseguridad de la Unión y convertir la ciberseguridad en una ventaja competitiva de otras industrias de la Unión, no pueden ser alcanzados de manera suficiente por los Estados miembros debido al hecho de que los recursos existentes son limitados y están dispersos, así como debido a la magnitud de las inversiones necesarias, sino que, a fin de evitar la duplicación innecesaria de

principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

los esfuerzos, ayudar a lograr una masa crítica de inversión y garantizar que la financiación pública se usa de forma óptima, pueden alcanzarse mejor a escala de la Unión. **Además, solo las acciones a escala de la Unión pueden garantizar el más alto nivel de ciberseguridad en todos los Estados miembros, colmando así las deficiencias en materia de seguridad que se dan en algunos Estados miembros y que dan lugar a deficiencias en materia de seguridad a escala de toda la Unión. Por tanto, la Unión** puede adoptar medidas, de **acuerdo** con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

## Enmienda 45

### Propuesta de Reglamento Artículo 1 – apartado 1

#### *Texto de la Comisión*

1. El presente Reglamento establece el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (en lo sucesivo, el «Centro de Competencia»), así como la Red de Centros Nacionales de Coordinación, y dispone las normas para la designación de los centros nacionales de coordinación y el establecimiento de la Comunidad de Competencias en Ciberseguridad.

#### *Enmienda*

1. El presente Reglamento establece el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (en lo sucesivo, el «Centro de Competencia»), así como la Red de Centros Nacionales de Coordinación, y dispone las normas para la designación de los centros nacionales de coordinación y el establecimiento de la Comunidad de Competencias en Ciberseguridad. **El Centro de Competencia y la Red contribuirán a la resiliencia y sensibilización general en la Unión con respecto a las amenazas para la ciberseguridad, teniendo plenamente en cuenta las implicaciones sociales.**

## Enmienda 46

### Propuesta de Reglamento

## Artículo 1 – apartado 3

*Texto de la Comisión*

*Enmienda*

3. *La sede del Centro de Competencia estará situada en [Bruselas (Bélgica)].*

*suprimido*

### Enmienda 47

#### Propuesta de Reglamento Artículo 1 – apartado 4

*Texto de la Comisión*

*Enmienda*

4. *El Centro de Competencia tendrá personalidad jurídica. Gozará en cada Estado miembro de la capacidad jurídica más amplia reconocida a las personas jurídicas por la legislación de dicho Estado. Podrá, en particular, adquirir o enajenar bienes muebles e inmuebles y ser parte en actuaciones judiciales.*

*suprimido*

### Enmienda 48

#### Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 1

*Texto de la Comisión*

*Enmienda*

1) «ciberseguridad», la protección de las redes y sistemas de información, sus usuarios y *otras* personas frente a las ciberamenazas;

1) «ciberseguridad», *todas las actividades necesarias para* la protección de las redes y sistemas de información, sus usuarios y *las* personas *afectadas* frente a las ciberamenazas;

### Enmienda 49

#### Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 2

*Texto de la Comisión*

*Enmienda*

2) «productos y *soluciones de ciberseguridad*», los productos, servicios o procesos de TIC destinados específicamente a proteger las redes y sistemas de información, así como a sus

2) «productos y *procesos*», los productos, servicios o procesos *comerciales y no comerciales* de TIC destinados específicamente a proteger *los datos*, las redes y sistemas de información,



usuarios y a **las** personas **afectadas**, frente a las **ciberamenazas**;

así como a sus usuarios y a **otras** personas, frente a las **amenazas para la ciberseguridad**;

## Enmienda 50

### Propuesta de Reglamento

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

*Texto de la Comisión*

*Enmienda*

**2 bis) «ciberamenaza», cualquier circunstancia, hecho o acción potencial que pueda dañar, perturbar o afectar desfavorablemente de otra manera a las redes y los sistemas de información, a sus usuarios y a las personas afectadas;**

## Enmienda 51

### Propuesta de Reglamento

#### Artículo 2 – párrafo 1 – punto 3

*Texto de la Comisión*

*Enmienda*

(3) «autoridad pública», cualquier Gobierno u otra administración pública, incluidos los organismos públicos consultivos, a nivel nacional, regional o local, o cualquier persona física o jurídica que desempeñe funciones administrativas públicas con arreglo al Derecho nacional, incluidas funciones específicas;

(3) «autoridad pública», cualquier Gobierno u otra administración pública, incluidos los organismos públicos consultivos, a nivel nacional, regional o local, o cualquier persona física o jurídica que desempeñe funciones administrativas públicas con arreglo al Derecho nacional **y de la Unión**, incluidas funciones específicas;

## Enmienda 52

### Propuesta de Reglamento

#### Artículo 2 – párrafo 1 – punto 4

*Texto de la Comisión*

*Enmienda*

(4) «Estado miembro **participante**», el Estado miembro que contribuye voluntariamente a sufragar los costes administrativos y de funcionamiento del Centro de Competencia.

(4) «Estado miembro **contribuyente**», el Estado miembro que contribuye voluntariamente a sufragar los costes administrativos y de funcionamiento del Centro de Competencia;

## Enmienda 53

### Propuesta de Reglamento

#### Artículo 2 – párrafo 1 – punto 4 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

**4 bis) «centro europeo de innovación digital», la entidad jurídica que se define en el Reglamento (UE) 2019/XXX del Parlamento Europeo y del Consejo<sup>1 bis</sup>.**

---

<sup>1 bis</sup> **Reglamento (UE) 2019/XXX del Parlamento Europeo y del Consejo, de ..., por el que se establece el programa Europa Digital para el período 2021-2027 (DO L [...] de [...], p. [...]) (2018/0227(COD)).**

## Enmienda 54

### Propuesta de Reglamento

#### Artículo 3 – apartado 1 – letra a

*Texto de la Comisión*

*Enmienda*

a) ***mantener*** y desarrollar las capacidades tecnológicas *e* industriales en materia de ciberseguridad necesarias para garantizar la protección de su mercado único digital;

a) desarrollar las capacidades y ***competencias*** tecnológicas, industriales, ***sociales, académicas y de investigación*** en materia de ciberseguridad necesarias para garantizar la protección de su mercado único digital ***y fomentar la protección de los datos de los ciudadanos, las empresas y las administraciones públicas de la Unión;***

## Enmienda 55

### Propuesta de Reglamento

#### Artículo 3 – apartado 1 – letra a bis (nueva)

*Texto de la Comisión*

*Enmienda*

***a bis) aumentar la resiliencia y la fiabilidad de las infraestructuras de las redes y los sistemas de información, incluidas las infraestructuras fundamentales, internet y los equipos y***

*programas informáticos de uso común en la Unión;*

## **Enmienda 56**

### **Propuesta de Reglamento Artículo 3 – apartado 1 – letra b**

*Texto de la Comisión*

b) aumentar la competitividad de la industria de ciberseguridad de la Unión y convertir la ciberseguridad en una ventaja competitiva para otras industrias de la Unión.

*Enmienda*

*(No afecta a la versión española).*

## **Enmienda 57**

### **Propuesta de Reglamento Artículo 3 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

***b bis) sensibilizar con respecto a las amenazas para la ciberseguridad, así como a las implicaciones e inquietudes sociales y éticas conexas, y reducir la brecha de capacidades en materia de ciberseguridad en la Unión;***

## **Enmienda 58**

### **Propuesta de Reglamento Artículo 3 – apartado 1 – letra b ter (nueva)**

*Texto de la Comisión*

*Enmienda*

***b ter) desarrollar el liderazgo europeo en materia de ciberseguridad y garantizar los niveles más elevados en ese ámbito en toda la Unión;***

## **Enmienda 59**

### **Propuesta de Reglamento Artículo 3 – apartado 1 – letra b quater (nueva)**

*Texto de la Comisión*

*Enmienda*

*b quater) reforzar la competitividad y las capacidades de la Unión al tiempo que se reduce su dependencia digital aumentando la asimilación de los productos, procesos y servicios de ciberseguridad desarrollados en la Unión;*

## **Enmienda 60**

### **Propuesta de Reglamento**

#### **Artículo 3 – apartado 1 – letra b quinquies (nueva)**

*Texto de la Comisión*

*Enmienda*

*b quinquies) reforzar la confianza de los ciudadanos, los consumidores y las empresas en el mundo digital, y contribuir, por ende, a los objetivos de la Estrategia para el Mercado Único Digital;*

## **Enmienda 61**

### **Propuesta de Reglamento**

#### **Artículo 4 – párrafo 1 – punto 1**

*Texto de la Comisión*

*Enmienda*

1. facilitar y *ayudar a coordinar la labor de* la Red de Centros Nacionales de Coordinación (en lo sucesivo, la «Red») a que se refiere el artículo 6 y de la Comunidad de Competencias en Ciberseguridad a que se refiere el artículo 8;

1. *crear, administrar* y facilitar la Red de Centros Nacionales de Coordinación (en lo sucesivo, la «Red») a que se refiere el artículo 6 y de la Comunidad de Competencias en Ciberseguridad (*en lo sucesivo, la «Comunidad»*) a que se refiere el artículo 8;

## **Enmienda 62**

### **Propuesta de Reglamento**

#### **Artículo 4 – párrafo 1 – punto 2**

*Texto de la Comisión*

*Enmienda*

2. *contribuir a* la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX<sup>26</sup>, y en particular de

2. *coordinar* la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX<sup>26</sup>, y en particular de

las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], y del programa Horizonte Europa, establecido por el Reglamento n.º XXX<sup>27</sup>, y en particular la sección 2.2.6 del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico], y de otros programas de la Unión cuando así se establezca en actos jurídicos de la Unión;

---

<sup>26</sup> [añadir título completo y referencia del DO]

<sup>27</sup> [añadir título completo y referencia del DO]

### Enmienda 63

#### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – parte introductoria

##### *Texto de la Comisión*

3. mejorar las capacidades, los conocimientos y las infraestructuras en materia de ciberseguridad al servicio de la industria, el sector público y la comunidad investigadora a través de lo siguiente:

### Enmienda 64

#### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra a

las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], y del programa Horizonte Europa, establecido por el Reglamento n.º XXX<sup>27</sup>, y en particular la sección 2.2.6 del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico], y de otros programas de la Unión cuando así se establezca en actos jurídicos de la Unión, **y contribuir a la ejecución de las acciones financiadas por el Fondo Europeo de Defensa establecido por el Reglamento (UE) 2019/XXX;**

---

<sup>26</sup> [añadir título completo y referencia del DO]

<sup>27</sup> [añadir título completo y referencia del DO]

##### *Enmienda*

3. mejorar **la resiliencia, las competencias**, las capacidades, los conocimientos y las infraestructuras en materia de ciberseguridad al servicio de **la sociedad**, la industria, el sector público y la comunidad investigadora, **habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos**, a través de lo siguiente:

*Texto de la Comisión*

a) **habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos**, adquirir **estas infraestructuras** y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión, desde la industria, **incluidas** las pymes, hasta el sector público y la comunidad científica e investigadora;

*Enmienda*

a) adquirir **las instalaciones del Centro de Competencia** y los servicios conexos, actualizarlos, explotarlos y ponerlos a disposición, **de manera equitativa, abierta y transparente**, de una amplia gama de usuarios en toda la Unión, desde la industria, **en particular** las pymes, hasta el sector público y la comunidad científica e investigadora;

**Enmienda 65**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 3 – letra a**

*Texto de la Comisión*

b) **habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos**, proporcionar apoyo a otras entidades, incluido de tipo financiero, para adquirir **estas infraestructuras** y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión, desde la industria, **incluidas** las pymes, hasta el sector público y la comunidad científica e investigadora;

*Enmienda*

b) proporcionar apoyo a otras entidades, incluido de tipo financiero, para adquirir **esas instalaciones** y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión, desde la industria, **en particular** las pymes, hasta el sector público y la comunidad científica e investigadora;

**Enmienda 66**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 3 – letra b bis (nueva)**

*Texto de la Comisión*

**b bis) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes, las pymes, las microempresas, las asociaciones, los expertos individuales y los proyectos de tecnología cívica del ámbito de la**

*Enmienda*

*ciberseguridad;*

## Enmienda 67

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra b ter (nueva)

*Texto de la Comisión*

*Enmienda*

*b ter) financiar auditorías de la codificación de la seguridad en los programas informáticos y las mejoras correspondientes en los proyectos de programas informáticos libres y de código abierto de uso común en infraestructuras, productos y procesos;*

## Enmienda 68

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra c

*Texto de la Comisión*

*Enmienda*

c) *proporcionar* conocimientos y asistencia técnica en materia de ciberseguridad *a* la industria *y a* las autoridades públicas, en particular apoyando las medidas destinadas a facilitar el acceso a los conocimientos especializados disponibles en la Red y en la Comunidad de Competencias en Ciberseguridad;

c) *facilitar el intercambio de* conocimientos y asistencia técnica en materia de ciberseguridad, *por ejemplo con la sociedad civil*, la industria, las autoridades públicas *y la comunidad académica e investigadora*, en particular apoyando las medidas destinadas a facilitar el acceso a los conocimientos especializados disponibles en la Red y en la Comunidad de Competencias en Ciberseguridad, *con el fin de mejorar la resiliencia cibernética en la Unión;*

## Enmienda 69

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra c bis (nueva)

*Texto de la Comisión*

*Enmienda*

*c bis) promover la «seguridad mediante el diseño» como principio en el proceso de desarrollo, mantenimiento, explotación y actualización de infraestructuras, productos y servicios, en particular*

*apoyando métodos de vanguardia de desarrollo seguro, pruebas de seguridad adecuadas y auditorías de seguridad, e incluyendo el compromiso de que los productores o proveedores pongan a disposición actualizaciones que subsanen las nuevas vulnerabilidades o amenazas, sin demora y más allá de la duración estimada de la vida útil del producto, o que permitan a un tercero crear y proporcionar dichas actualizaciones;*

## **Enmienda 70**

### **Propuesta de Reglamento**

#### **Artículo 4 – párrafo 1 – punto 3 – letra c ter (nueva)**

*Texto de la Comisión*

*Enmienda*

*c ter) respaldar las políticas de contribución al código fuente y su desarrollo, en particular cuando se trate de proyectos de programas informáticos libres y de código abierto utilizados por las autoridades públicas;*

## **Enmienda 71**

### **Propuesta de Reglamento**

#### **Artículo 4 – párrafo 1 – punto 3 – letra c quater (nueva)**

*Texto de la Comisión*

*Enmienda*

*c quater) agrupar a las partes interesadas de la industria, los sindicatos, el mundo académico, las organizaciones de investigación y las entidades públicas para garantizar la cooperación a largo plazo para el desarrollo y la implantación de los productos y procesos de ciberseguridad, lo que incluirá poner en común y compartir recursos e información en relación con dichos productos y procesos, si procede;*

## **Enmienda 72**

### **Propuesta de Reglamento**

#### **Artículo 4 – párrafo 1 – punto 4 – parte introductoria**



*Texto de la Comisión*

4. contribuir a una amplia implantación de productos y ***soluciones*** de ciberseguridad de última generación en ***todos los sectores de la economía*** a través de lo siguiente:

**Enmienda 73**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 4 – letra a**

*Texto de la Comisión*

a) estimular la investigación y el desarrollo en materia de ciberseguridad y la asimilación de los productos y ***soluciones*** de ciberseguridad de la Unión por parte de las autoridades públicas y ***las industrias usuarias***;

**Enmienda 74**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 4 – letra b**

*Texto de la Comisión*

b) ayudar a las autoridades públicas, a las industrias de la demanda y a otros usuarios a ***adoptar e integrar las últimas soluciones*** de ciberseguridad;

**Enmienda 75**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 4 – letra c**

*Texto de la Comisión*

c) apoyar en particular a las autoridades públicas en la organización de sus contratos públicos o llevar a cabo la contratación de productos y ***soluciones*** de

*Enmienda*

4. contribuir a una amplia implantación de productos y ***procesos*** de ciberseguridad ***sostenibles*** y de última generación en ***toda la Unión*** a través de lo siguiente:

*Enmienda*

a) estimular la investigación y el desarrollo en materia de ciberseguridad y la asimilación de los productos y ***procesos holísticos*** de ciberseguridad de la Unión ***a lo largo de todo el ciclo de innovación*** por parte, ***por ejemplo***, de las autoridades públicas, ***la industria y el mercado***;

*Enmienda*

b) ayudar a las autoridades públicas, a las industrias de la demanda y a otros usuarios a ***aumentar su resiliencia adoptando e integrando productos y procesos*** de ciberseguridad ***de última generación***;

*Enmienda*

c) apoyar en particular a las autoridades públicas en la organización de sus contratos públicos o llevar a cabo la contratación de productos y ***procesos*** de

ciberseguridad de vanguardia en nombre de las autoridades públicas;

ciberseguridad de vanguardia en nombre de las autoridades públicas, ***también mediante el apoyo a la contratación pública, con el fin de aumentar la seguridad y las ventajas de la inversión pública;***

## Enmienda 76

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 4 – letra d

##### *Texto de la Comisión*

d) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes y las pymes del ámbito de la ciberseguridad para que entren en contacto con mercados potenciales y atraigan inversiones;

##### *Enmienda*

d) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes, las pymes, ***las microempresas, los expertos individuales, los proyectos de programas informáticos libres y de código abierto de uso común, y los proyectos de tecnología cívica*** del ámbito de la ciberseguridad ***para mejorar los conocimientos especializados en materia de ciberseguridad*** y para que entren en contacto con mercados potenciales ***y oportunidades de implantación*** y atraigan inversiones;

## Enmienda 77

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 5 – parte introductoria

##### *Texto de la Comisión*

5. mejorar la comprensión de la ciberseguridad y contribuir a reducir el déficit de capacidades en la Unión en relación con la ciberseguridad a través de lo siguiente:

##### *Enmienda*

5. mejorar la comprensión de la ciberseguridad y contribuir a reducir el déficit de capacidades ***y a reforzar el nivel de capacitación*** en la Unión en relación con la ciberseguridad a través de lo siguiente:

## Enmienda 78

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 5 – letra -a (nueva)

**-a) apoyar, si procede, el logro del objetivo específico 4, «Competencias digitales avanzadas», del programa Europa Digital, en cooperación con los centros europeos de innovación digital;**

## Enmienda 79

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 5 – letra a

Texto de la Comisión

Enmienda

a) promover un mayor desarrollo de las capacidades en materia de ciberseguridad, **colaborando**, cuando proceda, con los órganos y organismos pertinentes de la UE, en particular la ENISA;

a) promover un mayor desarrollo, **puesta en común e intercambio** de las capacidades y **competencias** en materia de ciberseguridad **en todos los niveles educativos pertinentes, apoyar el objetivo de lograr el equilibrio de género, facilitar un elevado nivel común de conocimientos en materia de ciberseguridad, y contribuir a la resiliencia de los usuarios y las infraestructuras en toda la Unión en coordinación con la Red** y, cuando proceda, **en consonancia** con los órganos y organismos pertinentes de la UE, en particular la ENISA;

## Enmienda 80

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 6 – letra a

Texto de la Comisión

Enmienda

a) proporcionar apoyo financiero a los esfuerzos de investigación en materia de ciberseguridad sobre la base **de un programa** industrial, tecnológico y de investigación, de carácter estratégico, plurianual y común, sometido a una evaluación y mejora constantes;

a) proporcionar apoyo financiero a los esfuerzos de investigación en materia de ciberseguridad sobre la base **del plan** industrial, tecnológico y de investigación, de carácter estratégico, plurianual y común, sometido a una evaluación y mejora constantes, **a que se refiere el artículo 13;**

## Enmienda 81

**Propuesta de Reglamento**  
**Artículo 4 – párrafo 1 – punto 6 – letra b**

*Texto de la Comisión*

b) apoyar proyectos de investigación y demostración a gran escala relativos a las capacidades tecnológicas de ciberseguridad de próxima generación, en colaboración con la industria y la Red;

*Enmienda*

b) apoyar proyectos de investigación y demostración a gran escala relativos a las capacidades tecnológicas de ciberseguridad de próxima generación, en colaboración con la industria, **la comunidad académica e investigadora, el sector público y las autoridades públicas, incluidas la Red y la Comunidad;**

**Enmienda 82**

**Propuesta de Reglamento**  
**Artículo 4 – párrafo 1 – punto 6 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

***b bis) garantizar el respeto de los derechos fundamentales y una conducta ética en los proyectos de investigación en materia de ciberseguridad apoyados por el Centro de Competencia;***

**Enmienda 83**

**Propuesta de Reglamento**  
**Artículo 4 – párrafo 1 – punto 6 – letra b ter (nueva)**

*Texto de la Comisión*

*Enmienda*

***b ter) realizar un seguimiento de los informes de las vulnerabilidades detectadas por la Comunidad y facilitar la divulgación de las vulnerabilidades, el desarrollo de parches, rectificaciones y soluciones y su distribución;***

**Enmienda 84**

**Propuesta de Reglamento**  
**Artículo 4 – párrafo 1 – punto 6 – letra b quater (nueva)**

*Texto de la Comisión*

*Enmienda*

***b quater) realizar un seguimiento de los resultados de las investigaciones relativas a los algoritmos autodidactas empleados en actividades informáticas malintencionadas, en colaboración con la ENISA y en apoyo de la aplicación de la Directiva (UE) 2016/1148;***

#### **Enmienda 85**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 6 – letra b quinquies (nueva)**

*Texto de la Comisión*

*Enmienda*

***b quinquies) apoyar la investigación en el ámbito de la ciberdelincuencia;***

#### **Enmienda 86**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 6 – letra b sexies (nueva)**

*Texto de la Comisión*

*Enmienda*

***b sexies) apoyar la investigación y el desarrollo de productos y procesos que puedan ser estudiados, compartidos y aprovechados libremente, particularmente en el ámbito de los equipos y programas informáticos verificados y verificables, en estrecha cooperación con la industria, la Red y la Comunidad;***

#### **Enmienda 87**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 6 – letra c**

*Texto de la Comisión*

*Enmienda*

c) apoyar la investigación y la innovación en aras de la normalización en el ámbito de la tecnología de ciberseguridad;

c) apoyar la investigación y la innovación en aras de la normalización y ***certificación formal y no formal*** en el ámbito de la tecnología de ciberseguridad, ***estableciendo una conexión con los***

*trabajos existentes y, en su caso, en estrecha cooperación con las organizaciones de normalización europeas, los organismos de certificación y la ENISA;*

#### **Enmienda 88**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 6 – letra c bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*c bis) prestar un apoyo especial a las pymes facilitándoles el acceso a conocimientos y formación mediante un acceso a su medida a los resultados finales de la investigación y el desarrollo reforzados por el Centro de Competencia y la Red a fin de aumentar la competitividad;*

#### **Enmienda 89**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 8 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*b bis) asistir y proporcionar asesoramiento a la Comisión en relación con la aplicación del Reglamento (UE) 2019/XXX [refundición del Reglamento (CE) n.º 428/2009 de conformidad con la propuesta COM(2016)0616];*

#### **Enmienda 90**

##### **Propuesta de Reglamento**

##### **Artículo 4 – párrafo 1 – punto 8 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*8 bis. contribuir a los esfuerzos de la Unión por reforzar la cooperación internacional en materia de ciberseguridad a través de lo siguiente:*

*a) facilitar la participación del*

*Centro de Competencia en conferencias internacionales y organizaciones gubernamentales así como la contribución a las organizaciones internacionales de normalización;*

*b) cooperar con terceros países y organizaciones internacionales en el contexto de los marcos de cooperación internacional pertinentes;*

## **Enmienda 91**

### **Propuesta de Reglamento Artículo 5 – título**

#### *Texto de la Comisión*

Inversión en y utilización de infraestructuras, capacidades, productos o ***soluciones***

#### *Enmienda*

Inversión en y utilización de infraestructuras, capacidades, productos o ***procesos***

## **Enmienda 92**

### **Propuesta de Reglamento Artículo 5 – apartado 1 – parte introductoria**

#### *Texto de la Comisión*

1. Cuando el Centro de Competencia financie infraestructuras, capacidades, productos o ***soluciones*** con arreglo al artículo 4, apartados 3 y 4, en forma de subvención o premio, el plan de trabajo del Centro de Competencia podrá especificar en particular lo siguiente:

#### *Enmienda*

1. Cuando el Centro de Competencia financie infraestructuras, capacidades, productos o ***procesos*** con arreglo al artículo 4, apartados 3 y 4, en forma de ***contrato público***, subvención o premio, el plan de trabajo del Centro de Competencia podrá especificar en particular lo siguiente:

## **Enmienda 93**

### **Propuesta de Reglamento Artículo 5 – apartado 1 – letra a**

#### *Texto de la Comisión*

a) las normas por las que se regirá la explotación de una infraestructura o capacidad, incluida, en su caso, la asignación de la explotación a una entidad anfitriona sobre la base de los criterios que

#### *Enmienda*

a) las normas ***específicas*** por las que se regirá la explotación de una infraestructura o capacidad, incluida, en su caso, la asignación de la explotación a una entidad anfitriona sobre la base de los

el Centro de Competencia defina;

critérios que el Centro de Competencia defina;

#### Enmienda 94

##### Propuesta de Reglamento

##### Artículo 5 – apartado 1 – letra b bis (nueva)

*Texto de la Comisión*

*Enmienda*

***b bis) las normas específicas por las que se regirán las distintas fases de ejecución;***

#### Enmienda 95

##### Propuesta de Reglamento

##### Artículo 5 – apartado 1 – letra b ter (nueva)

*Texto de la Comisión*

*Enmienda*

***b ter) que, como resultado de la contribución de la Unión, el acceso sea tan abierto como sea posible y tan restringido como sea necesario, y que sea posible la reutilización;***

#### Enmienda 96

##### Propuesta de Reglamento

##### Artículo 5 – apartado 2

*Texto de la Comisión*

*Enmienda*

2. El Centro de Competencia podrá ser responsable de la ejecución global de las correspondientes medidas de contratación conjunta, en particular las contrataciones precomerciales en nombre de los miembros de la Red, ***los miembros de la Comunidad de Competencias en Ciberseguridad u otras terceras partes que representen a los usuarios de productos y soluciones de ciberseguridad.*** A tal fin, el Centro de Competencia podrá estar asistido por uno o varios centros nacionales de coordinación ***o*** miembros de la Comunidad de Competencias en Ciberseguridad.

2. El Centro de Competencia podrá ser responsable de la ejecución global de las correspondientes medidas de contratación conjunta, en particular las contrataciones precomerciales en nombre de los miembros de la Red. A tal fin, el Centro de Competencia podrá estar asistido por uno o varios centros nacionales de coordinación, miembros de la Comunidad de Competencias en Ciberseguridad ***o centros europeos de innovación digital pertinentes.***



## Enmienda 97

### Propuesta de Reglamento Artículo 6 – apartado -1 (nuevo)

*Texto de la Comisión*

*Enmienda*

**-1. En cada Estado miembro se creará un centro nacional de coordinación.**

## Enmienda 98

### Propuesta de Reglamento Artículo 6 – apartado 4

*Texto de la Comisión*

*Enmienda*

4. El centro nacional de coordinación designado deberá tener la capacidad de apoyar al Centro de Competencia y a la Red en el cumplimiento de su misión, según se establece en el artículo 3 del presente Reglamento. Asimismo, deberá poseer o tener acceso directo a conocimientos tecnológicos especializados en ciberseguridad y estar en condiciones de comprometerse y coordinarse eficazmente con la industria, el sector público y la comunidad investigadora.

4. El centro nacional de coordinación designado deberá tener la capacidad de apoyar al Centro de Competencia y a la Red en el cumplimiento de su misión, según se establece en el artículo 3 del presente Reglamento. Asimismo, deberá poseer o tener acceso directo a conocimientos tecnológicos especializados en ciberseguridad y estar en condiciones de comprometerse y coordinarse eficazmente con la industria, el sector público, la comunidad **académica e** investigadora y los ciudadanos. **La Comisión publicará directrices en las que se detallará el procedimiento de evaluación y se explicará la aplicación de los criterios.**

## Enmienda 99

### Propuesta de Reglamento Artículo 6 – apartado 5

*Texto de la Comisión*

*Enmienda*

5. La relación entre el Centro de Competencia y los centros nacionales de coordinación se basará en un acuerdo contractual firmado entre el Centro de Competencia y cada uno de los centros nacionales de coordinación. El acuerdo **establecerá** las normas por las que se regirán las relaciones y el reparto de

5. La relación entre el Centro de Competencia y los centros nacionales de coordinación se basará en un acuerdo contractual **estándar** firmado entre el Centro de Competencia y cada uno de los centros nacionales de coordinación. El acuerdo **consistirá en un mismo conjunto de condiciones generales armonizadas**

funciones entre el Centro de Competencia y cada centro nacional de coordinación.

**que establezca** las normas por las que se regirán las relaciones y el reparto de funciones entre el Centro de Competencia y cada centro nacional de coordinación y **las condiciones especiales adaptadas al centro nacional de coordinación de que se trate.**

## Enmienda 100

### Propuesta de Reglamento

#### Artículo 6 – apartado 5 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

**5 bis. A fin de complementar el presente Reglamento, la Comisión adoptará actos delegados con arreglo al artículo 45 bis por los que se definan las condiciones generales armonizadas de los acuerdos contractuales a que se refiere el apartado 5 del presente artículo, en particular su formato.**

## Enmienda 101

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra a

*Texto de la Comisión*

*Enmienda*

a) apoyar al Centro de Competencia en pos de la consecución de sus objetivos, y en particular en lo referente a la coordinación de la Comunidad de Competencias en Ciberseguridad;

a) apoyar al Centro de Competencia en pos de la consecución de sus objetivos, y en particular en lo referente **al establecimiento y** a la coordinación de la Comunidad de Competencias en Ciberseguridad;

## Enmienda 102

### Propuesta de Reglamento

#### Artículo 1 – apartado 1 – letra b

*Texto de la Comisión*

*Enmienda*

b) **facilitar** la participación de la industria y **de** otros agentes a nivel de los Estados miembros en proyectos

b) **promover, fomentar y facilitar** la participación de la **sociedad civil, la** industria, **en particular las empresas**

transfronterizos;

*emergentes y las pymes, la comunidad académica e investigadora y otros agentes a nivel de los Estados miembros en proyectos transfronterizos;*

### **Enmienda 103**

#### **Propuesta de Reglamento**

#### **Artículo 7 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*b bis) en cooperación con otras entidades que tengan funciones similares, servir de ventanilla única para los productos y procesos de ciberseguridad financiados con cargo a otros programas como InvestEU o el Programa sobre el Mercado Único, en particular para las pymes;*

### **Enmienda 104**

#### **Propuesta de Reglamento**

#### **Artículo 1 – apartado 1 – letra c**

*Texto de la Comisión*

*Enmienda*

c) contribuir, junto con el Centro de Competencia, a identificar y hacer frente a los retos *industriales* en materia de ciberseguridad específicos de cada sector;

c) contribuir, junto con el Centro de Competencia, a identificar y hacer frente a los retos en materia de ciberseguridad específicos de cada sector;

### **Enmienda 105**

#### **Propuesta de Reglamento**

#### **Artículo 1 – apartado 1 – letra c bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*c bis) cooperar estrechamente con las organizaciones nacionales de normalización para promover la adopción de las normas en vigor e involucrar a todas las partes interesadas pertinentes, en particular a las pymes, en la definición*

*de normas nuevas;*

## **Enmienda 106**

### **Propuesta de Reglamento**

#### **Artículo 7 – apartado 1 – letra e**

*Texto de la Comisión*

e) tratar de establecer sinergias con las actividades oportunas a nivel nacional y regional;

*Enmienda*

e) tratar de establecer sinergias con las actividades oportunas a nivel nacional, regional y **local**;

## **Enmienda 107**

### **Propuesta de Reglamento**

#### **Artículo 7 – apartado 1 – letra f bis (nueva)**

*Texto de la Comisión*

*Enmienda*

***f bis) promover y difundir programas educativos comunes mínimos en materia de ciberseguridad en cooperación con los organismos pertinentes de los Estados miembros;***

## **Enmienda 108**

### **Propuesta de Reglamento**

#### **Artículo 1 – apartado 1 – letra g**

*Texto de la Comisión*

g) promover y difundir los resultados pertinentes de la labor de la Red, la Comunidad de Competencias en Ciberseguridad y el Centro de Competencia a nivel nacional o regional;

*Enmienda*

g) promover y difundir los resultados pertinentes de la labor de la Red, la Comunidad de Competencias en Ciberseguridad y el Centro de Competencia a nivel nacional, regional o **local**;

## **Enmienda 109**

### **Propuesta de Reglamento**

#### **Artículo 1 – apartado 1 – letra h**

*Texto de la Comisión*

h) evaluar las solicitudes de las entidades establecidas en el mismo Estado miembro que el centro de coordinación para formar parte de la Comunidad de Competencias en Ciberseguridad.

*Enmienda*

h) evaluar las solicitudes de las entidades **y personas** establecidas en el mismo Estado miembro que el centro de coordinación para formar parte de la Comunidad de Competencias en Ciberseguridad.

**Enmienda 110**

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

*Texto de la Comisión*

4. Los centros nacionales de coordinación cooperarán, **cuando proceda**, a través de la Red a fin de realizar las funciones mencionadas en el apartado 1, **letras a), b), c), e) y g)**.

*Enmienda*

4. Los centros nacionales de coordinación, **cuando proceda**, cooperarán a través de la Red **y se coordinarán con los centros europeos de innovación digital pertinentes** a fin de realizar las funciones mencionadas en el apartado 1.

**Enmienda 111**

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

*Texto de la Comisión*

1. La Comunidad de Competencias en Ciberseguridad **contribuirá** a la misión del Centro de Competencia, según se establece en el artículo 3, **y reforzará y difundirá** los conocimientos especializados en materia de ciberseguridad en toda la Unión.

*Enmienda*

1. La Comunidad de Competencias en Ciberseguridad **contribuye** a la misión del Centro de Competencia, según se establece en el artículo 3, **refuerza, pone en común, comparte y difunde** los conocimientos especializados en materia de ciberseguridad en toda la Unión **y proporciona conocimientos técnicos especializados**.

**Enmienda 112**

**Propuesta de Reglamento**  
**Artículo 8 – apartado 2**

*Texto de la Comisión*

2. La Comunidad de Competencias en Ciberseguridad estará compuesta por la industria, **organizaciones de investigación del ámbito universitario y sin ánimo de lucro**, asociaciones y entidades públicas y **otras entidades** que se ocupen de cuestiones operativas y técnicas. Reunirá a las principales partes interesadas en relación con las capacidades tecnológicas **e industriales** en materia de ciberseguridad **de** la Unión. Contará con la participación de los centros nacionales de coordinación, **así como** las instituciones y los organismos de la Unión que dispongan de los conocimientos especializados pertinentes.

*Enmienda*

2. La Comunidad de Competencias en Ciberseguridad estará compuesta por la **sociedad civil, la industria tanto de la demanda como de la oferta, incluidas las pymes, la comunidad académica e investigadora, las asociaciones de usuarios, expertos individuales, las organizaciones europeas de normalización pertinentes y otras** asociaciones y entidades públicas y **de otra índole** que se ocupen de cuestiones operativas y técnicas **en el ámbito de la ciberseguridad**. Reunirá a las principales partes interesadas en relación con las capacidades **y competencias** tecnológicas, **industriales, académicas y de investigación y sociales** en materia de ciberseguridad **en** la Unión **y** contará con la participación de los centros nacionales de coordinación, **los centros europeos de innovación digital** y las instituciones y los organismos de la Unión que dispongan de los conocimientos especializados pertinentes, **como se contempla en el artículo 10 del presente Reglamento**.

**Enmienda 113**

**Propuesta de Reglamento**

**Artículo 8 – apartado 3 – parte introductoria**

*Texto de la Comisión*

3. Solo las entidades establecidas en la Unión podrán ser acreditadas como miembros de la Comunidad de Competencias en Ciberseguridad. Deberán demostrar que **poseen** conocimientos técnicos en materia de ciberseguridad en al menos uno de los ámbitos siguientes:

*Enmienda*

3. Solo las entidades establecidas **y las personas residentes** en la Unión, **el Espacio Económico Europeo (EEE) o la Asociación Europea de Libre Comercio (AELC)** podrán ser acreditadas como miembros de la Comunidad de Competencias en Ciberseguridad. **Los solicitantes** deberán demostrar que **pueden proporcionar** conocimientos técnicos en materia de ciberseguridad en al menos uno de los ámbitos siguientes:

## Enmienda 114

### Propuesta de Reglamento Artículo 8 – apartado 3 – letra a

*Texto de la Comisión*

a) investigación;

*Enmienda*

a) **ámbito académico o** investigación;

## Enmienda 115

### Propuesta de Reglamento Artículo 8 – apartado 3 – letra c bis (nueva)

*Texto de la Comisión*

*Enmienda*

**c bis) ética;**

## Enmienda 116

### Propuesta de Reglamento Artículo 8 – apartado 3 – letra c ter (nueva)

*Texto de la Comisión*

*Enmienda*

**c ter) normalización y especificaciones formales y técnicas;**

## Enmienda 117

### Propuesta de Reglamento Artículo 8 – apartado 4

*Texto de la Comisión*

*Enmienda*

4. El Centro de Competencia acreditará a las entidades establecidas con arreglo a la legislación nacional como miembros de la Comunidad de Competencias en Ciberseguridad, previa evaluación realizada por el centro nacional de coordinación del Estado miembro en el que esté establecida la entidad acerca del cumplimiento de los criterios establecidos

4. El Centro de Competencia acreditará a las **personas o a las** entidades establecidas con arreglo a la legislación nacional como miembros de la Comunidad de Competencias en Ciberseguridad, previa evaluación **armonizada** realizada por el Centro **de Competencia y por el centro** nacional de coordinación del Estado miembro en el que esté establecida la

en el apartado 3 por parte de dicha entidad. La acreditación no tendrá una duración limitada, pero podrá ser revocada por el Centro de Competencia en cualquier momento si este o el centro nacional de coordinación pertinente considera que la entidad no cumple los criterios establecidos en el apartado 3 o entra en el ámbito de aplicación de las correspondientes disposiciones del artículo 136 del Reglamento XXX [nuevo Reglamento Financiero].

entidad *o resida la persona* acerca del cumplimiento de los criterios establecidos en el apartado 3 por parte de dicha entidad *o persona*. La acreditación no tendrá una duración limitada, pero podrá ser revocada por el Centro de Competencia en cualquier momento si este o el centro nacional de coordinación pertinente considera que la entidad *o la persona* no cumple los criterios establecidos en el apartado 3 o entra en el ámbito de aplicación de las correspondientes disposiciones del artículo 136 del Reglamento XXX [nuevo Reglamento Financiero]. *Los centros nacionales de coordinación de los Estados miembros procurarán lograr una representación equilibrada de las partes interesadas en la Comunidad, fomentando activamente la participación de categorías y colectivos infrarrepresentados, como las pymes.*

## Enmienda 118

### Propuesta de Reglamento Artículo 8 – apartado 4 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

*4 bis. A fin de complementar el presente Reglamento, la Comisión adoptará actos delegados con arreglo al artículo 45 bis por los que se especifiquen los criterios de selección de los solicitantes previstos en el apartado 3 del presente artículo y los procedimientos para evaluar y acreditar a las entidades que cumplan los criterios a que se refiere el apartado 4 del presente artículo.*

## Enmienda 119

### Propuesta de Reglamento Artículo 9 – párrafo 1 – punto 5 bis (nuevo)



**5 bis) apoyarán al Centro de Competencia comunicando y divulgando vulnerabilidades, ayudando a mitigarlas y proporcionando asesoramiento para reducirlas, también mediante la certificación con arreglo a los regímenes adoptados de conformidad con el Reglamento (UE) 2019/XXX [el Reglamento de Ciberseguridad].**

## Enmienda 120

### Propuesta de Reglamento Artículo 10 – apartado 1

Texto de la Comisión

1. El Centro de Competencia cooperará con las instituciones, órganos y organismos correspondientes de la Unión, en particular la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE), el Servicio Europeo de Acción Exterior, el Centro Común de Investigación de la Comisión, la Agencia Ejecutiva de Investigación, la Agencia Ejecutiva de Innovación y Redes, el Centro Europeo de Ciberdelincuencia de Europol y la Agencia Europea de Defensa.

Enmienda

1. **Para garantizar la coherencia y la complementariedad**, el Centro de Competencia cooperará con las instituciones, órganos y organismos correspondientes de la Unión, en particular la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (**ENISA**), el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE), el Servicio Europeo de Acción Exterior, el Centro Común de Investigación de la Comisión, la Agencia Ejecutiva de Investigación, la Agencia Ejecutiva de Innovación y Redes, **los centros europeos de innovación digital pertinentes**, el Centro Europeo de Ciberdelincuencia de Europol y la Agencia Europea de Defensa **en lo referente a los proyectos, servicios y competencias de doble uso**.

## Enmienda 121

### Propuesta de Reglamento Artículo 10 – apartado 2

*Texto de la Comisión*

2. La cooperación se llevará a cabo en el marco de convenios de trabajo. Estos convenios **se someterán a** la aprobación previa de la Comisión.

*Enmienda*

2. La cooperación se llevará a cabo en el marco de convenios de trabajo. Estos convenios **serán adoptados por el Consejo de Administración tras** la aprobación previa de la Comisión.

**Enmienda 122**

**Propuesta de Reglamento  
Artículo 12 – apartado 1**

*Texto de la Comisión*

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y **cinco** representantes de la Comisión, en nombre de la Unión.

*Enmienda*

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro, **un representante designado como observador por el Parlamento Europeo y cuatro** representantes de la Comisión, en nombre de la Unión, **procurando alcanzar el equilibrio de género entre los miembros y sus suplentes.**

**Enmienda 123**

**Propuesta de Reglamento  
Artículo 12 – apartado 3**

*Texto de la Comisión*

3. Los miembros del Consejo de Administración y sus suplentes serán nombrados en función de sus conocimientos en el ámbito **tecnológico**, así como las correspondientes capacidades en materia de presupuestos, administración y gestión. La Comisión y los Estados miembros procurarán limitar la rotación de sus representantes en el Consejo de Administración con el fin de garantizar la continuidad en la labor de este órgano. La Comisión y los Estados miembros tratarán de lograr una representación equilibrada entre hombres y mujeres en el Consejo de

*Enmienda*

3. Los miembros del Consejo de Administración y sus suplentes serán nombrados en función de sus conocimientos en el ámbito **de la ciberseguridad**, así como las correspondientes capacidades en materia de presupuestos, administración y gestión. La Comisión y los Estados miembros procurarán limitar la rotación de sus representantes en el Consejo de Administración con el fin de garantizar la continuidad en la labor de este órgano. La Comisión y los Estados miembros tratarán de lograr una representación equilibrada

Administración.

entre hombres y mujeres en el Consejo de Administración.

#### Enmienda 124

##### Propuesta de Reglamento Artículo 12 – apartado 6

###### *Texto de la Comisión*

6. **La Comisión** podrá invitar observadores, incluidos representantes de los órganos y organismos de la Unión pertinentes, para que participen en **las** reuniones **del Consejo de Administración**, cuando proceda.

###### *Enmienda*

6. **El Consejo de Administración** podrá invitar **a** observadores, incluidos representantes de los órganos y organismos de la Unión pertinentes, **y a los miembros de la Comunidad** para que participen en **sus** reuniones, cuando proceda.

#### Enmienda 125

##### Propuesta de Reglamento Artículo 12 – apartado 7

###### *Texto de la Comisión*

7. La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) **será un observador permanente del** Consejo de Administración.

###### *Enmienda*

7. La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) **y el Consejo Consultivo Industrial y Científico serán observadores permanentes en el** Consejo de Administración **en calidad de asesores sin derecho de voto. El Consejo de Administración tendrá en cuenta en la mayor medida posible las opiniones de los observadores permanentes.**

#### Enmienda 126

##### Propuesta de Reglamento Artículo 13 – apartado 3 – letra a

###### *Texto de la Comisión*

a) adoptará un plan estratégico plurianual que contendrá una declaración de las principales prioridades e iniciativas previstas del Centro de Competencia,

###### *Enmienda*

a) adoptará un plan estratégico plurianual que contendrá una declaración de las principales prioridades e iniciativas previstas del Centro de Competencia,

incluida una estimación de las necesidades y fuentes de financiación;

incluida una estimación de las necesidades y fuentes de financiación, ***teniendo en cuenta el asesoramiento proporcionado por la ENISA***;

#### **Enmienda 127**

##### **Propuesta de Reglamento Artículo 3 – apartado 3 – letra b**

###### *Texto de la Comisión*

b) aprobará el plan de trabajo, las cuentas anuales, el balance y el informe anual de actividades del Centro de Competencia, sobre la base de una propuesta del director ejecutivo;

###### *Enmienda*

b) aprobará el plan de trabajo, las cuentas anuales, el balance y el informe anual de actividades del Centro de Competencia, sobre la base de una propuesta del director ejecutivo, ***teniendo en cuenta el asesoramiento proporcionado por la ENISA***;

#### **Enmienda 128**

##### **Propuesta de Reglamento Artículo 13 – apartado 3 – letra e**

###### *Texto de la Comisión*

e) adoptará los ***criterios y*** procedimientos para evaluar y acreditar a las entidades como miembros de la Comunidad de Competencias en Ciberseguridad;

###### *Enmienda*

e) adoptará los procedimientos para evaluar y acreditar a las entidades como miembros de la Comunidad de Competencias en Ciberseguridad;

#### **Enmienda 129**

##### **Propuesta de Reglamento Artículo 13 – apartado 3 – letra e bis (nueva)**

###### *Texto de la Comisión*

###### *Enmienda*

***e bis) adoptará los convenios de trabajo a que se refiere el artículo 10, apartado 2;***

#### **Enmienda 130**

**Propuesta de Reglamento**  
**Artículo 13 – apartado 3 – letra g bis (nueva)**

*Texto de la Comisión*

*Enmienda*

***g bis) adoptará normas de transparencia para el Centro de Competencia;***

**Enmienda 131**

**Propuesta de Reglamento**  
**Artículo 13 – apartado 3 – letra i**

*Texto de la Comisión*

*Enmienda*

i) creará grupos de trabajo con miembros de la Comunidad de Competencias en Ciberseguridad;

i) creará grupos de trabajo con miembros de la Comunidad de Competencias en Ciberseguridad;  
***teniendo en cuenta el asesoramiento proporcionado por los observadores permanentes;***

**Enmienda 132**

**Propuesta de Reglamento**  
**Artículo 13 – apartado 3 – letra l**

*Texto de la Comisión*

*Enmienda*

l) promocionará *el* Centro de Competencia ***en todo el mundo a fin de aumentar su atractivo y convertirlo en un organismo de categoría mundial por su excelencia en materia de ciberseguridad;***

l) promocionará ***la cooperación del*** Centro de Competencia ***con agentes globales;***

**Enmienda 133**

**Propuesta de Reglamento**  
**Artículo 13 – apartado 3 – letra r**

*Texto de la Comisión*

*Enmienda*

r) adoptará una estrategia contra el fraude que esté en consonancia con el riesgo de fraude, teniendo en cuenta el análisis ***coste-beneficio*** de las medidas que

r) adoptará una estrategia contra el fraude ***y la corrupción*** que esté en consonancia con el riesgo de fraude ***y corrupción***, teniendo en cuenta el análisis

vayan a aplicarse;

*costes-beneficio* de las medidas que vayan a aplicarse, *así como medidas exhaustivas para la protección de las personas que informen sobre infracciones del Derecho de la Unión, con arreglo a la legislación aplicable de la Unión;*

#### Enmienda 134

##### Propuesta de Reglamento Artículo 13 – apartado 3 – letra s

###### *Texto de la Comisión*

s) adoptará *la* metodología para calcular *la contribución financiera* de los Estados miembros;

###### *Enmienda*

s) adoptará *una definición amplia de las contribuciones financieras de los Estados miembros y una* metodología para calcular *el importe de las contribuciones voluntarias* de los Estados miembros *que puedan contabilizarse como contribuciones financieras según esta definición. Este cálculo se efectuará al final de cada ejercicio presupuestario;*

#### Enmienda 135

##### Propuesta de Reglamento Artículo 14 – apartado 1

###### *Texto de la Comisión*

1. El Consejo de Administración elegirá a un presidente o presidenta y a un vicepresidente o vicepresidenta de entre los miembros con derecho de voto, para un período de dos años. El mandato del presidente y del vicepresidente podrá prorrogarse una vez, previa decisión del Consejo de Administración. No obstante, si el presidente o el vicepresidente dejaran de ser miembros del Consejo de Administración durante su mandato, este expirará automáticamente en la misma fecha. El vicepresidente sustituirá de oficio al presidente cuando este no pueda desempeñar sus funciones. El presidente

###### *Enmienda*

1. El Consejo de Administración elegirá a un presidente o presidenta y a un vicepresidente o vicepresidenta de entre los miembros con derecho de voto, para un período de dos años, *procurando alcanzar el equilibrio de género*. El mandato del presidente y del vicepresidente podrá prorrogarse una vez, previa decisión del Consejo de Administración. No obstante, si el presidente o el vicepresidente dejaran de ser miembros del Consejo de Administración durante su mandato, este expirará automáticamente en la misma fecha. El vicepresidente sustituirá de oficio al presidente cuando este no pueda desempeñar sus funciones. El presidente

participará en las votaciones.

participará en las votaciones.

### **Enmienda 136**

#### **Propuesta de Reglamento Artículo 14 – apartado 3**

##### *Texto de la Comisión*

3. El director ejecutivo participará en las deliberaciones, salvo decisión contraria del Consejo de Administración, pero no tendrá derecho de voto. ***El Consejo de Administración podrá, de manera puntual, invitar a otras personas a asistir a sus reuniones en calidad de observadores.***

##### *Enmienda*

3. El director ejecutivo participará en las deliberaciones, salvo decisión contraria del Consejo de Administración, pero no tendrá derecho de voto.

### **Enmienda 137**

#### **Propuesta de Reglamento Artículo 14 – apartado 4**

##### *Texto de la Comisión*

4. ***Los miembros del Consejo Consultivo Industrial y Científico, previa invitación del presidente, podrán participar en las reuniones del Consejo de Administración, sin derecho de voto.***

##### *Enmienda*

***suprimido***

### **Enmienda 138**

#### **Propuesta de Reglamento Artículo 15**

##### *Texto de la Comisión*

##### ***Artículo 15***

##### ***Normas de votación en el Consejo de Administración***

1. ***La Unión poseerá el 50 % de los derechos de voto. Los derechos de voto de la Unión serán indivisibles.***

##### *Enmienda*

***suprimido***

2. *Cada Estado miembro participante tendrá un voto.*

3. *El Consejo de Administración tomará sus decisiones por mayoría de al menos el 75 % de todos los votos – incluidos los de los miembros ausentes– que representen al menos el 75 % del total de las contribuciones financieras al Centro de Competencia. La contribución financiera se calculará a partir de las estimaciones de gastos propuestas por los Estados miembros a que se refiere el artículo 17, apartado 2, letra c), y del informe sobre el valor de las contribuciones de los Estados miembros participantes a que se refiere el artículo 22, apartado 5.*

4. *Solo los representantes de la Comisión y los representantes de los Estados miembros participantes tendrán derecho de voto.*

5. *El presidente participará en las votaciones.*

## **Enmienda 139**

### **Propuesta de Reglamento Artículo 15 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

#### *Artículo 15 bis*

#### *Normas de votación en el Consejo de Administración*

1. *Las decisiones que se sometan a votación podrán referirse a lo siguiente:*
  - a) *gobernanza y organización del Centro de Competencia y la Red;*
  - b) *asignación de presupuesto al Centro de Competencia y a la Red;*
  - c) *acciones conjuntas de varios Estados miembros, complementadas en su caso, tras una decisión, por recursos de la Unión asignados con arreglo a la letra b).*



2. *El Consejo de Administración tomará sus decisiones por mayoría de al menos el 75 % de todos los votos, incluidos los votos de los miembros ausentes. Los derechos de voto de la Unión estarán representados por la Comisión y serán indivisibles.*

3. *Para las decisiones contempladas en el apartado 1, letra a), cada Estado miembro estará representado y tendrá los mismos derechos de voto. Para los votos restantes disponibles hasta llegar al 100 %, la Unión deberá tener al menos el 50 % de los derechos de voto correspondientes a su contribución financiera.*

4. *Para las decisiones contempladas en el apartado 1, letras b) o c), o cualquier otra decisión que no esté contemplada en las categorías del apartado 1, la Unión poseerá al menos el 50 % de los derechos de voto correspondientes a su contribución financiera. Solo los Estados miembros contribuyentes tendrán derechos de voto, que corresponderán a su contribución financiera.*

5. *En caso de que el presidente haya sido elegido de entre los representantes de los Estados miembros, participará en las votaciones como representante de su Estado miembro.*

## Enmienda 140

### Propuesta de Reglamento Artículo 16 – apartado 3

#### *Texto de la Comisión*

3. El Consejo de Administración nombrará al director ejecutivo a partir de una lista de candidatos propuesta por la Comisión después de un procedimiento de selección abierto y *transparente*.

#### *Enmienda*

3. El Consejo de Administración nombrará al director ejecutivo a partir de una lista de candidatos propuesta por la Comisión, *que incluya candidatos designados por los Estados miembros con vistas a alcanzar el equilibrio de género*, después de un procedimiento de selección

abierto, *transparente* y *no discriminatorio*.

#### **Enmienda 141**

##### **Propuesta de Reglamento Artículo 16 – apartado 5**

###### *Texto de la Comisión*

5. El mandato del director ejecutivo tendrá una duración de **cuatro** años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las tareas y los desafíos futuros del Centro de Competencia.

###### *Enmienda*

5. El mandato del director ejecutivo tendrá una duración de **cinco** años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las tareas y los desafíos futuros del Centro de Competencia.

#### **Enmienda 142**

##### **Propuesta de Reglamento Artículo 16 – apartado 6**

###### *Texto de la Comisión*

6. A propuesta de la Comisión, que tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá ampliar una vez el mandato del director ejecutivo, por un plazo máximo de **cuatro** años.

###### *Enmienda*

6. A propuesta de la Comisión, que tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá ampliar una vez el mandato del director ejecutivo, por un plazo máximo de **cinco** años.

#### **Enmienda 143**

##### **Propuesta de Reglamento Artículo 16 – apartado 8**

###### *Texto de la Comisión*

8. El director ejecutivo solo podrá ser cesado mediante decisión del Consejo de Administración, a propuesta de la Comisión.

###### *Enmienda*

8. El director ejecutivo solo podrá ser cesado mediante decisión del Consejo de Administración, a propuesta de **sus miembros o de** la Comisión.

#### **Enmienda 144**

**Propuesta de Reglamento**  
**Artículo 17 – apartado 2 – letra c**

*Texto de la Comisión*

c) previa consulta al Consejo de Administración y a la Comisión, elaborar y presentar al Consejo de Administración, para su adopción, el proyecto de plan estratégico plurianual y el proyecto de plan de trabajo anual del Centro de Competencia, incluido el ámbito de aplicación de las convocatorias de propuestas, las convocatorias de manifestaciones de interés y las licitaciones necesarias para ejecutar el plan de trabajo, así como las correspondientes estimaciones de gastos propuestas por los Estados miembros y la Comisión;

*Enmienda*

c) previa consulta al Consejo de Administración, **al Consejo Consultivo Industrial y Científico, a la ENISA** y a la Comisión, elaborar y presentar al Consejo de Administración, para su adopción, el proyecto de plan estratégico plurianual y el proyecto de plan de trabajo anual del Centro de Competencia, incluido el ámbito de aplicación de las convocatorias de propuestas, las convocatorias de manifestaciones de interés y las licitaciones necesarias para ejecutar el plan de trabajo, así como las correspondientes estimaciones de gastos propuestas por los Estados miembros y la Comisión;

**Enmienda 145**

**Propuesta de Reglamento**  
**Artículo 17 – apartado 2 – letra h**

*Texto de la Comisión*

h) elaborar un plan de actuación sobre la base de las conclusiones de las evaluaciones retrospectivas e informar a la Comisión cada dos años de los progresos al respecto;

*Enmienda*

h) elaborar un plan de actuación sobre la base de las conclusiones de las evaluaciones retrospectivas e informar a la Comisión **y al Parlamento Europeo** cada dos años de los progresos al respecto;

**Enmienda 146**

**Propuesta de Reglamento**  
**Artículo 17 – apartado 2 – letra l**

*Texto de la Comisión*

l) aprobar la lista de acciones seleccionadas para su financiación sobre la base de la clasificación establecida por un grupo de expertos independientes;

*Enmienda*

l) aprobar, **previa consulta al Consejo Consultivo Industrial y Científico y a la ENISA**, la lista de acciones seleccionadas para su financiación sobre la base de la clasificación establecida por un grupo de

expertos independientes;

#### Enmienda 147

##### Propuesta de Reglamento Artículo 17 – apartado 2 – letra s

###### *Texto de la Comisión*

s) elaborar un plan de actuación sobre la base de las conclusiones de los informes de las auditorías internas o externas, así como de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF), y presentar informes sobre los progresos realizados, dos veces al año a la Comisión y periódicamente al Consejo de Administración;

###### *Enmienda*

s) elaborar un plan de actuación sobre la base de las conclusiones de los informes de las auditorías internas o externas, así como de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF), y presentar informes sobre los progresos realizados, dos veces al año a la Comisión y **al Parlamento Europeo** y periódicamente al Consejo de Administración;

#### Enmienda 148

##### Propuesta de Reglamento Artículo 17 – apartado 2 – letra v

###### *Texto de la Comisión*

v) garantizar una comunicación eficaz con las instituciones de la Unión;

###### *Enmienda*

v) garantizar una comunicación eficaz con las instituciones de la Unión **e informar a Consejo al Parlamento Europeo y al Consejo cuando lo soliciten;**

#### Enmienda 149

##### Propuesta de Reglamento Artículo 18 – apartado 1

###### *Texto de la Comisión*

1. El Consejo Consultivo Industrial y Científico tendrá un máximo de **dieciséis** miembros. Los miembros serán nombrados por el Consejo de Administración de entre los representantes de las entidades de la Comunidad **de Competencias en**

###### *Enmienda*

1. El Consejo Consultivo Industrial y Científico tendrá un máximo de **veinticinco** miembros. Los miembros serán nombrados por el Consejo de Administración de entre los representantes de las entidades de la Comunidad **o sus miembros individuales. Solo podrán optar a ser miembros los**

**Ciberseguridad.**

***representantes de entidades que no estén controladas por un tercer país o una entidad de un tercer país, a menos que el país pertenezca al EEE o la AELC. El nombramiento se realizará de conformidad con un procedimiento de selección abierto, transparente y no discriminatorio. En la composición del Consejo se procurará alcanzar el equilibrio de género, así como lograr una representación equilibrada de los grupos de partes interesadas de la industria, la comunidad académica y la sociedad civil.***

## **Enmienda 150**

### **Propuesta de Reglamento Artículo 18 – apartado 2**

#### *Texto de la Comisión*

2. Los miembros del Consejo Consultivo Industrial y Científico tendrán conocimientos especializados en materia de investigación sobre ciberseguridad, desarrollo industrial, ***servicios profesionales*** o implantación de servicios profesionales. El Consejo de Administración especificará con más detalle los requisitos acerca de dichos conocimientos especializados.

#### *Enmienda*

2. Los miembros del Consejo Consultivo Industrial y Científico tendrán conocimientos especializados en materia de investigación sobre ciberseguridad, desarrollo industrial ***y oferta, ejecución o implantación de servicios o productos*** profesionales. El Consejo de Administración especificará con más detalle los requisitos acerca de dichos conocimientos especializados.

## **Enmienda 151**

### **Propuesta de Reglamento Artículo 18 – apartado 5**

#### *Texto de la Comisión*

5. Los representantes de la Comisión y de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea ***podrán*** apoyar ***y participar en*** la labor del Consejo Consultivo Industrial y Científico.

#### *Enmienda*

5. ***Se invitará a*** los representantes de la Comisión y de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea ***a*** apoyar la labor del Consejo Consultivo Industrial y Científico ***y participar en ella. El Consejo podrá invitar a otros representantes de la Comunidad en calidad de observadores,***

*asesores o expertos, cuando proceda y según el caso.*

## **Enmienda 152**

### **Propuesta de Reglamento Artículo 19 – apartado 1**

#### *Texto de la Comisión*

1. El Consejo Consultivo Industrial y Científico se reunirá como mínimo **dos** veces al año.

#### *Enmienda*

1. El Consejo Consultivo Industrial y Científico se reunirá como mínimo **tres** veces al año.

## **Enmienda 153**

### **Propuesta de Reglamento Artículo 19 – apartado 2**

#### *Texto de la Comisión*

2. El Consejo Consultivo Industrial y Científico **podrá asesorar** al Consejo de Administración acerca de la creación de grupos de trabajo sobre cuestiones específicas de interés para la labor del Centro de Competencia, cuando sea necesario bajo la coordinación general de uno o varios miembros del Consejo Consultivo Industrial y Científico.

#### *Enmienda*

2. El Consejo Consultivo Industrial y Científico **hará sugerencias** al Consejo de Administración acerca de la creación de grupos de trabajo sobre cuestiones específicas de interés para la labor del Centro de Competencia, **cuando estas cuestiones correspondan a las tareas y los ámbitos de competencia descritos en el artículo 20** y cuando sea necesario bajo la coordinación general de uno o varios miembros del Consejo Consultivo Industrial y Científico.

## **Enmienda 154**

### **Propuesta de Reglamento Artículo 20 – párrafo 1 – parte introductoria**

#### *Texto de la Comisión*

El Consejo Consultivo Industrial y Científico asesorará al Centro de Competencia respecto del desempeño de sus actividades y deberá:

#### *Enmienda*

El Consejo Consultivo Industrial y Científico asesorará **regularmente** al Centro de Competencia respecto del desempeño de sus actividades y deberá:

## Enmienda 155

### Propuesta de Reglamento

#### Artículo 20 – párrafo 1 – punto 1

##### *Texto de la Comisión*

1) proporcionar asesoramiento estratégico al director ejecutivo y al Consejo de Administración y aportarles su contribución a efectos de la elaboración del plan de trabajo y del plan estratégico plurianual dentro de los plazos fijados por el Consejo de Administración;

##### *Enmienda*

1) proporcionar asesoramiento estratégico al director ejecutivo y al Consejo de Administración y aportarles su contribución a efectos de la ***implantación por el Centro de Competencia y la orientación y las operaciones de este por lo que respecta a la industria y la ciencia, así como de la*** elaboración del plan de trabajo y del plan estratégico plurianual dentro de los plazos fijados por el Consejo de Administración;

## Enmienda 156

### Propuesta de Reglamento

#### Artículo 20 – párrafo 1 – punto 1 bis (nuevo)

##### *Texto de la Comisión*

##### *Enmienda*

***1 bis) asesorar al Consejo de Administración sobre la creación de grupos de trabajo sobre cuestiones específicas relacionadas con el trabajo del Centro de Competencia;***

## Enmienda 157

### Propuesta de Reglamento

#### Artículo 20 – párrafo 1 – punto 3

##### *Texto de la Comisión*

##### *Enmienda*

3) promover y recabar observaciones sobre el plan de trabajo y el plan estratégico plurianual del Centro de Competencia.

3) promover y recabar observaciones sobre el plan de trabajo y el plan estratégico plurianual del Centro de Competencia, ***así como asesorar al Consejo de Administración sobre el modo de mejorar la orientación estratégica y el***

## **Enmienda 158**

### **Propuesta de Reglamento Artículo 21 – apartado 1 – letra a**

*Texto de la Comisión*

a) **1 981 668 000 EUR** con cargo al programa Europa Digital, incluidos hasta **23 746 000 EUR** para gastos administrativos;

*Enmienda*

a) **1 780 954 875 EUR a precios de 2018 (1 998 696 000 EUR a precios corrientes)** con cargo al programa Europa Digital, incluidos hasta **21 385 465 EUR a precios de 2018 (23 746 000 EUR a precios corrientes)** para gastos administrativos;

## **Enmienda 159**

### **Propuesta de Reglamento Artículo 21 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

**b bis) un importe del Fondo Europeo de Defensa para acciones del Centro de Competencia relacionadas con la defensa, incluidos todos los costes administrativos relacionados, como aquellos en que el Centro pueda incurrir cuando actúe como director de proyecto en acciones amparadas por el Fondo Europeo de Defensa.**

## **Enmienda 160**

### **Propuesta de Reglamento Artículo 21 – apartado 2**

*Texto de la Comisión*

*Enmienda*

2. La contribución máxima de la Unión se abonará con cargo a los créditos del presupuesto general de la Unión asignados al [programa Europa Digital] y

2. La contribución máxima de la Unión se abonará con cargo a los créditos del presupuesto general de la Unión asignados al [programa Europa Digital], al



al Programa Específico por el que se ejecuta Horizonte Europa, establecido por la Decisión XXX.

Programa Específico por el que se ejecuta Horizonte Europa, establecido por la Decisión XXX, ***al Fondo Europeo de Defensa y a otros programas y proyectos comprendidos en el ámbito de competencias del Centro de Competencia o la Red.***

## Enmienda 161

### Propuesta de Reglamento Artículo 21 – apartado 4

#### *Texto de la Comisión*

4. La contribución financiera de la Unión no cubrirá las funciones mencionadas en el artículo 4, apartado 8, letra b).

#### *Enmienda*

4. La contribución financiera de la Unión ***con cargo al programa Europa Digital y al programa Horizonte Europa*** no cubrirá las funciones mencionadas en el artículo 4, apartado 8, letra b). ***Estas funciones se podrán cubrir con contribuciones del Fondo Europeo de Defensa.***

## Enmienda 162

### Propuesta de Reglamento Artículo 22 – apartado 4

#### *Texto de la Comisión*

4. La Comisión podrá poner fin, reducir proporcionalmente o suspender la contribución financiera de la Unión al Centro de Competencia en caso de que los Estados miembros participantes no aporten, aporten solo parcialmente ***o aporten con retraso*** las contribuciones a que se refiere el apartado 1.

#### *Enmienda*

4. La Comisión podrá poner fin, reducir proporcionalmente o suspender la contribución financiera de la Unión al Centro de Competencia en caso de que los Estados miembros participantes no aporten ***o*** aporten solo parcialmente las contribuciones a que se refiere el apartado 1. ***La supresión, reducción o suspensión por parte de la Comisión de la contribución financiera de la Unión será proporcional, en cuanto al importe y el plazo, a la reducción, supresión o suspensión de las contribuciones de los Estados miembros.***

## Enmienda 163

### Propuesta de Reglamento

#### Artículo 23 – apartado 4 – letra a

##### *Texto de la Comisión*

a) las contribuciones financieras de los Estados miembros participantes a los gastos administrativos;

##### *Enmienda*

a) las contribuciones financieras de **la Unión y de** los Estados miembros participantes a los gastos administrativos;

## Enmienda 164

### Propuesta de Reglamento

#### Artículo 23 – apartado 4 – letra b

##### *Texto de la Comisión*

b) las contribuciones financieras de los Estados miembros participantes a los gastos de funcionamiento;

##### *Enmienda*

b) las contribuciones financieras de **la Unión y de** los Estados miembros participantes a los gastos de funcionamiento;

## Enmienda 165

### Propuesta de Reglamento

#### Artículo 23 – apartado 8 bis (nuevo)

##### *Texto de la Comisión*

##### *Enmienda*

**8 bis. El Centro de Competencia cooperará estrechamente con otras instituciones, órganos y organismos de la Unión a fin de aprovechar las sinergias y de reducir, cuando proceda, los costes administrativos.**

## Enmienda 166

### Propuesta de Reglamento

#### Artículo 30 – apartado 1

##### *Texto de la Comisión*

1. El Centro de Competencia adoptará las medidas adecuadas para garantizar que,

##### *Enmienda*

1. El Centro de Competencia adoptará las medidas adecuadas para garantizar que,

cuando se realicen las acciones financiadas en el marco del presente Reglamento, los intereses financieros de la Unión queden protegidos mediante la aplicación de medidas preventivas contra el fraude, la corrupción y cualquier otra actividad ilegal, mediante controles eficaces y, en caso de detectarse irregularidades, mediante la recuperación de las cantidades abonadas indebidamente y, cuando proceda, la imposición de sanciones administrativas eficaces, proporcionadas y disuasorias.

cuando se realicen las acciones financiadas en el marco del presente Reglamento, los intereses financieros de la Unión queden protegidos mediante la aplicación de medidas preventivas contra el fraude, la corrupción y cualquier otra actividad ilegal, mediante controles **regulares y** eficaces y, en caso de detectarse irregularidades, mediante la recuperación de las cantidades abonadas indebidamente y, cuando proceda, la imposición de sanciones administrativas eficaces, proporcionadas y disuasorias.

## Enmienda 167

### Propuesta de Reglamento Artículo 31 – apartado 7

#### *Texto de la Comisión*

7. El **personal del** Centro de Competencia estará formado por agentes temporales y agentes contratados.

#### *Enmienda*

7. El Centro de Competencia **procurará alcanzar el equilibrio de género entre su personal. El personal** estará formado por agentes temporales y agentes contratados.

## Enmienda 168

### Propuesta de Reglamento Artículo 34 – apartado 2 – letra c bis (nueva)

#### *Texto de la Comisión*

#### *Enmienda*

**c bis) Los artículos 22 [Titularidad de los resultados], 23 [Titularidad de los resultados] y 30 [Aplicación de las normas en materia de información clasificada] del Reglamento (UE) 2019/XXX [Fondo Europeo de Defensa] se aplicarán a la participación del Centro de Competencia en todas las acciones relacionadas con la defensa; cuando esté previsto en el plan de trabajo, y la concesión de licencias no exclusivas podrá limitarse a terceros que estén establecidos o que se considere que están**

*establecidos en los Estados miembros y que estén controlados por los Estados miembros o por nacionales de los Estados miembros.*

## Enmienda 169

### Propuesta de Reglamento Artículo 35 – apartado 1

#### *Texto de la Comisión*

1. El Centro de Competencia realizará todas sus actividades con **un alto** grado de transparencia.

#### *Enmienda*

1. El Centro de Competencia realizará todas sus actividades con **el máximo** grado de transparencia.

## Enmienda 170

### Propuesta de Reglamento Artículo 35 – apartado 2

#### *Texto de la Comisión*

2. El Centro de Competencia 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** labor. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 41.

#### *Enmienda*

2. El Centro de Competencia velará por que **se facilite a su debido tiempo al** público y **a** las partes interesadas **información completa**, adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de **la** labor **del Centro de Competencia, la Red, el Consejo Consultivo Industrial y Científico y la Comunidad**. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 42.

## Enmienda 171

### Propuesta de Reglamento Artículo 38 – apartado 3

#### *Texto de la Comisión*

3. La evaluación a que se refiere el apartado 2 incluirá un balance de los resultados alcanzados por el Centro de

#### *Enmienda*

3. La evaluación a que se refiere el apartado 2 incluirá un balance de los resultados alcanzados por el Centro de

Competencia, a la vista de sus objetivos, su **mandato y sus funciones**. Si la Comisión considera que la continuidad del Centro de Competencia está justificada con respecto a los objetivos, el mandato y las funciones que le han sido asignados, podrá proponer que se amplíe la duración del mandato del Centro de Competencia establecida en el artículo 46.

Competencia, a la vista de sus objetivos, **mandato y funciones, su eficacia y su eficiencia**. Si la Comisión considera que la continuidad del Centro de Competencia está justificada con respecto a los objetivos, el mandato y las funciones que le han sido asignados, podrá proponer que se amplíe la duración del mandato del Centro de Competencia establecida en el artículo 46.

## Enmienda 172

### Propuesta de Reglamento Artículo 38 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

#### **Artículo 38 bis**

#### **Personalidad jurídica del Centro de Competencia**

- 1. El Centro de Competencia tendrá personalidad jurídica.**
- 2. Gozará en cada Estado miembro de la capacidad jurídica más amplia reconocida a las personas jurídicas por la legislación de dicho Estado miembro. Podrá, en particular, adquirir o enajenar bienes muebles e inmuebles y personarse en procedimientos judiciales.**

## Enmienda 173

### Propuesta de Reglamento Artículo 42 – párrafo 1

*Texto de la Comisión*

*Enmienda*

El Consejo de Administración del Centro de Competencia adoptará normas para la prevención y **gestión** de los conflictos de intereses en relación con sus miembros, sus órganos o su personal. **Dichas normas contendrán disposiciones destinadas a evitar los conflictos de intereses en**

El Consejo de Administración del Centro de Competencia adoptará normas para la prevención, **detección y resolución** de los conflictos de intereses en relación con sus miembros, sus órganos o su personal, **incluidos el director ejecutivo, el Consejo de Administración, el Consejo Consultivo**

***relación con los representantes de los miembros que formen parte del Consejo de Administración, así como el Consejo Consultivo Industrial y Científico, de conformidad con el Reglamento XXX [nuevo Reglamento Financiero].***

Industrial y Científico y ***la Comunidad.***

#### **Enmienda 174**

**Propuesta de Reglamento  
Artículo 42 – párrafo 1 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***Los Estados miembros garantizarán la prevención, la detección y la resolución de los conflictos de intereses en relación con los centros nacionales de coordinación.***

#### **Enmienda 175**

**Propuesta de Reglamento  
Artículo 42 – párrafo 1 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

***Las normas mencionadas en el párrafo primero cumplirán lo dispuesto en el Reglamento (UE, Euratom) 2018/1046.***

#### **Enmienda 176**

**Propuesta de Reglamento  
Artículo 44 – título**

*Texto de la Comisión*

*Enmienda*

Apoyo del Estado miembro anfitrión

***Sede y apoyo del Estado miembro anfitrión***

#### **Enmienda 177**

**Propuesta de Reglamento  
Artículo 44 – párrafo -1 (nuevo)**

*Texto de la Comisión*

*Enmienda*

***La sede del Centro de Competencia se determinará mediante un procedimiento democráticamente responsable, aplicando criterios transparentes y de conformidad con el Derecho de la Unión.***

## **Enmienda 178**

### **Propuesta de Reglamento Artículo 44 – párrafo -1 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***El Estado miembro anfitrión ofrecerá las mejores condiciones posibles para garantizar el buen funcionamiento del Centro de Competencia, lo que incluye una sede única, además de otras condiciones como la accesibilidad de los 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 sus hijos y parejas.***

## **Enmienda 179**

### **Propuesta de Reglamento Artículo 44 – párrafo 1**

*Texto de la Comisión*

*Enmienda*

***Podrá celebrarse*** un convenio administrativo entre el Centro de Competencia y el Estado miembro ***[Bélgica]*** en el que esté establecida su sede en relación con los privilegios e inmunidades y otro tipo de apoyo que deba conceder dicho Estado miembro al Centro de Competencia.

***Se celebrará*** un convenio administrativo entre el Centro de Competencia y el Estado miembro ***anfitrión*** en el que esté establecida su sede en relación con los privilegios e inmunidades y otro tipo de apoyo que deba conceder dicho Estado miembro al Centro de Competencia.

## **Enmienda 180**

**Artículo 45 bis**

***Ejercicio de la delegación***

- 1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.***
- 2. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 5 bis, y en el artículo 8, apartado 4 ter, se otorgan a la Comisión por un período de tiempo indefinido a partir del ... [fecha de entrada en vigor del presente Reglamento].***
- 3. La delegación de poderes mencionada en el artículo 6, apartado 5 bis, y el artículo 8, apartado 4 ter, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.***
- 4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.***
- 5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.***
- 6. Los actos delegados adoptados en virtud del artículo 6, apartado 5 bis, y del artículo 8, apartado 4 ter, entrarán en***



*vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.*

## EXPOSICIÓN DE MOTIVOS

La propuesta de la Comisión por la que se establece un Centro de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación constituyen una excelente oportunidad para diseñar el futuro de la cooperación europea en materia de ciberseguridad.

De forma similar a otras partes de la economía europea, la innovación, los productos, los procesos y los servicios en materia de ciberseguridad se crean en gran medida en las pequeñas y medianas empresas. La innovación, cuando no se produce en estas pymes, tiene lugar en las empresas emergentes y en la comunidad investigadora. Estas comunidades, orientadas al sector económico, cuentan con el apoyo de empresarios individuales y, muy a menudo, de impulsos importantes procedentes de la sociedad civil y de proyectos de tecnología cívica precomerciales o no comerciales que hacen uso de normas abiertas, datos abiertos y *software* libre y de código abierto para contribuir al bien común.

Debemos asegurarnos de que el marco europeo de la ciberseguridad aproveche las oportunidades y los puntos fuertes que puede aportar el sector, tal como está estructurado actualmente en Europa.

La configuración propuesta del Centro vincula las actividades de Horizonte Europa para la investigación en materia de ciberseguridad y de Europa Digital para la implantación de la ciberseguridad, creando así idealmente sinergias y efectos indirectos entre ambos programas de la Unión. Por otra parte, el Centro ha de facilitar y coordinar la labor de la Red de Competencias en materia de Ciberseguridad e impulsar el programa tecnológico de ciberseguridad y facilitar el acceso a los conocimientos especializados reunidos en la Red y en la Comunidad. La Comisión consideró que la mejor manera de alcanzar estos objetivos era crear un nuevo órgano de la Unión que incluyera elementos de una empresa común, una agencia ejecutiva y una agencia descentralizada. Dado que con la ENISA ya existe otra agencia específica de ciberseguridad de la Unión, la presente propuesta debe garantizar que se consulte a la ENISA sobre todas las actividades pertinentes del Centro, a fin de crear sinergias.

### La ciberseguridad como proceso

La industria de la tecnología de la información utiliza desde hace mucho el término «solución» para describir productos y servicios en los contextos de las relaciones públicas y los apoyos comerciales. Sin embargo, es importante entender la ciberseguridad como un proceso. En la misma medida que evoluciona constantemente la tecnología de las TIC, también lo hacen las amenazas. Los esfuerzos por hacer más seguras nuestras infraestructuras, redes y sistemas de información no terminan con la compra de un determinado producto o servicio.

Por esta razón, es importante reforzar constantemente la ciberseguridad a lo largo de todo el ciclo de vida de un producto, y tener en cuenta la interacción de los productos y los agentes en redes e infraestructuras conectadas, como Internet. A lo largo de las fases del ciclo de vida de un sistema, el diseño, la ejecución, el mantenimiento y la fase de actualización, la seguridad debe ser un principio fundamental.

## Seguridad de la infraestructura común

Internet es la infraestructura común de la que depende cada vez más no solo la economía europea, sino también la mundial. Además, es la infraestructura común de comunicación, cultura e información de la que las personas dependen diariamente.

Desde la capa de infraestructura básica hasta las aplicaciones con las que interactúan los usuarios, el *software* libre y de código abierto desempeña un papel fundamental en el funcionamiento de Internet. Al igual que ocurre con cualquier componente utilizado habitualmente, si se descubre una vulnerabilidad en materia de seguridad en un componente de *software* libre y de código abierto, dicha vulnerabilidad puede amenazar el funcionamiento de Internet y de los servicios conexos.

Ya se sabe que se utilizan dispositivos vulnerables del «internet de las cosas» para atacar a otras infraestructuras. En Internet, una vulnerabilidad en materia de seguridad en un dispositivo de consumo puede afectar a un sistema informático de alto rendimiento.

Estos componentes son generalmente desarrollados, utilizados y construidos por los distintos agentes industriales, en la investigación y el desarrollo, así como por organismos públicos. Por consiguiente, con el fin de mejorar la fiabilidad general, la resiliencia y la seguridad de nuestra infraestructura común, las actividades del Centro deben realizar la función de *software* libre y de código abierto de uso común, y contribuir a su seguridad.

La resiliencia en lugar de la defensa y las tecnologías de doble uso

Debido al funcionamiento de las redes y de los sistemas de información, como Internet, no suele ser posible atribuir el origen de un ataque a una entidad con absoluta certeza. Al contrario, pueden fabricarse pruebas para encubrir una fuente o para inducir a conclusiones erróneas. En este contexto, es especialmente preocupante el hecho de que los Estados y las organizaciones intergubernamentales hayan empezado a considerar el uso de la fuerza militar convencional en caso de ciberataques.

Es una prioridad de la Unión Europea promover la democracia, el Estado de Derecho, los derechos humanos y las libertades fundamentales en todo el mundo. Por lo tanto, el Centro debe promover e invertir en la resiliencia y la integridad de las redes y los sistemas de información. Los productos y procesos de ciberseguridad pueden ser igualmente útiles en contextos civiles y militares, por lo que el Centro debe apoyar los marcos existentes para el control de las tecnologías de doble uso. Las aplicaciones militares ofensivas, como las «puertas traseras», las vulnerabilidades retenidas o los programas intrusos conllevan un riesgo de seguridad intrínseco para la sociedad en general, y serían contrarias al objetivo del Centro de mejorar la ciberseguridad. Por lo tanto, es importante limitar las actividades del Centro a fines civiles.

El hecho de que las estructuras y los costes de funcionamiento del Centro se financien con cargo a programas de la Unión que no pueden utilizarse con fines militares significa que el Centro no debe facilitar ninguna investigación en materia de defensa ni otros proyectos relacionados con la defensa. Deben respetarse los Tratados y el presupuesto de la Unión no debe utilizarse para fines militares.

## Sociedad, ética y representación

El Centro debe tener muy en cuenta las implicaciones y preocupaciones sociales y éticas que puedan entrañar sus acciones, las acciones de sus órganos y los resultados de los productos, servicios, instalaciones e investigaciones financiados por él.

Más que otras industrias, el sector de las TIC está luchando para satisfacer la demanda de trabajadores cualificados. Al mismo tiempo, la representación de hombres y mujeres, la diversidad étnica y las personas con discapacidad es extraordinariamente desequilibrada. Por ello, redunda en interés de la industria, incluidos el mundo académico, la investigación y otros, lograr una representación equilibrada.

Más aún, redunda en beneficio de la igualdad.

## Estructura de gobierno

El Centro y sus órganos deben velar por que los conflictos de intereses no solo se identifiquen, sino que se subsanen de manera transparente y responsable. Los Estados miembros deben asegurarse de que lo mismo se aplique a los centros nacionales de coordinación.

El Parlamento Europeo debe estar en pie de igualdad con los Estados miembros a la hora de influir en la gobernanza y las acciones del Centro.

## **ANEXO: LISTA DE LAS ORGANIZACIONES O PERSONAS QUE HAN COLABORADO CON LA PONENTE**

La lista siguiente se elabora con carácter totalmente voluntario y bajo la exclusiva responsabilidad de la ponente. Las siguientes organizaciones o personas han colaborado con la ponente durante la preparación del informe, hasta su adopción en comisión:

<b>Organización o persona</b>
American Chamber of Commerce to the EU
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)
CyberSec4Europe
Digitaleurope
European Cyber Security Organisation (ECSO)
European Defence Agency (EDA)
European DIGITAL SME Alliance
European Organisation for Security (EOS)
European Union Agency for Network and Information Security (ENISA)
FSFE - Free Software Foundation Europe e.V.
Huawei Technologies
Interel European Affairs
ISACA
KIT - Karlsruhe Institute of Technology, SecUnity project
Mozilla Corp.
Symantec Corp.

31.1.2019

## **OPINIÓN DE LA COMISIÓN DE MERCADO INTERIOR Y PROTECCIÓN DEL CONSUMIDOR**

para la Comisión de Industria, Investigación y Energía

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

Ponente de opinión: Arndt Kohn

### **BREVE JUSTIFICACIÓN**

En la era digital, la ciberseguridad es una parte esencial de la competitividad económica y la seguridad de la Unión Europea, así como de la integridad y los procesos que sustentan nuestras sociedades democráticas. Garantizar un alto grado de ciberresiliencia en toda la Unión reviste una importancia fundamental para conseguir la confianza de los consumidores en el mercado único digital y seguir impulsando una Europa más innovadora y competitiva. Aunque haya más de seiscientos centros en la Unión Europea que ofrecen conocimientos especializados en el ámbito de la ciberseguridad, la Unión sigue siendo un importador neto de productos y soluciones de ciberseguridad. Es necesario que la Unión muestre mayor unidad y eficacia a la hora de luchar contra los ciberataques, reforzando sus competencias en materia de ciberseguridad e incrementando su capacidad para proteger mejor a los ciudadanos, las empresas y las instituciones públicas de Europa.

En septiembre de 2017, la Comisión presentó el «Reglamento de Ciberseguridad», seguido por la propuesta para el establecimiento del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (en lo sucesivo, «Centro») y la Red de Centros Nacionales de Coordinación (en lo sucesivo, «Red») el 12 de septiembre de 2018.

En general, el ponente de opinión acoge favorablemente la propuesta de la Comisión. Se hace especial hincapié en los objetivos del Centro de Competencia de contribuir al mantenimiento y el desarrollo de las capacidades tecnológicas e industriales de ciberseguridad de la Unión, así como de reforzar la industria de la ciberseguridad de la Unión y aumentar su competitividad, lo que es compartido por el ponente de opinión. El Centro de Competencia facilitará y ayudará a coordinar la labor de la Red de Centros Nacionales de Coordinación y

de la Comunidad de Competencias en Ciberseguridad. El ponente de opinión prevé que el Centro de Competencia y la Red se utilicen como instrumento para fomentar la confianza de los ciudadanos europeos, así como para reforzar el mercado único digital.

No obstante, el ponente de opinión hace hincapié en que hay una serie de puntos de la propuesta que se deben clarificar y mejorar.

- En primer lugar, el ponente de opinión cree firmemente que los procesos de **acreditación y evaluación** que permiten a las entidades convertirse en miembros de la Comunidad deben **armonizarse a escala de la Unión** con el fin de evitar la fragmentación entre las diferentes entidades acreditadas por los distintos Estados miembros.
- En segundo lugar, hay que señalar **la importancia de las pymes** al objeto de mejorar la igualdad de oportunidades para ellas y reforzar su capacidad de participación y su competitividad en el mercado único. En este sentido, el objetivo del ponente de opinión es lograr una representación equilibrada de las partes interesadas en la Comunidad y en el Consejo Consultivo Industrial y Científico, prestando especial atención a la inclusión de las pymes. Además, en su opinión, los centros nacionales de coordinación también deben trabajar en estrecha cooperación para incentivar proyectos transfronterizos en el ámbito de la ciberseguridad, en particular para las pymes.
- En tercer lugar, el ponente de opinión está firmemente convencido de que el aumento de la adopción de los productos y soluciones de ciberseguridad creados en la Unión debe ser una de las misiones del Centro y de la Red, junto con el aumento de la competitividad de la industria de la ciberseguridad de la Unión. Para alcanzar estos objetivos, aclara **qué entidades pueden ser acreditadas como miembros de la Comunidad de Competencias en Ciberseguridad** y aboga por el refuerzo de la normalización europea en el ámbito de la tecnología de ciberseguridad.
- En cuarto lugar, por lo que se refiere a **las contribuciones financieras de los Estados miembros**, el ponente de opinión considera que la Comisión Europea no debe tener la facultad de poner fin a la contribución financiera de la Unión al Centro de Competencia, ni tampoco de reducirla proporcionalmente ni suspenderla. La Comisión propone hacer uso de esta facultad en el caso de que un Estado miembro contribuyente no aporte, aporte solo parcialmente o aporte con retraso las contribuciones, pero tal facultad penalizaría a toda la estructura que está creando el presente Reglamento y disuadiría a los Estados miembros de participar.
- Por último, el ponente de opinión destaca la importancia de crear una **sólida base de cibercapacidades** que también incluya campañas de formación y sensibilización.

## ENMIENDAS

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

### Enmienda 1

#### Propuesta de Reglamento Considerando 1

##### *Texto de la Comisión*

(1) *A medida que* nuestra vida cotidiana y la economía se **vuelven** más dependientes de las tecnologías digitales, los ciudadanos **están** cada vez más expuestos a incidentes cibernéticos graves. La seguridad futura depende, entre otras cosas, de la mejora de la capacidad tecnológica e industrial para proteger a la Unión frente a las ciberamenazas, ya que tanto la infraestructura civil como las capacidades militares dependen de unos sistemas digitales seguros.

##### *Enmienda*

(1) **Más del 80 % de la población de la Unión Europea está conectada a internet,** y nuestra vida cotidiana y la economía se **están volviendo** más dependientes de las tecnologías digitales, **con** los ciudadanos cada vez más expuestos a incidentes cibernéticos graves. La seguridad futura depende, entre otras cosas, de la mejora de la capacidad tecnológica e industrial para proteger a la Unión frente a las ciberamenazas, ya que tanto la infraestructura civil como las capacidades militares dependen de unos sistemas digitales seguros.

### Enmienda 2

#### Propuesta de Reglamento Considerando 4

##### *Texto de la Comisión*

(4) En la Cumbre Digital de Tallin, celebrada en septiembre de 2017, los jefes de Estado y de Gobierno pidieron que la Unión se convirtiera en «un líder mundial en ciberseguridad para 2025, a fin de garantizar la confianza, la seguridad y la protección de nuestros ciudadanos, consumidores y empresas en línea y permitir una Internet libre y legal».

##### *Enmienda*

(4) En la Cumbre Digital de Tallin, celebrada en septiembre de 2017, los jefes de Estado y de Gobierno pidieron que la Unión se convirtiera en un líder mundial en ciberseguridad para 2025, a fin de garantizar la confianza, la seguridad y la protección de nuestros ciudadanos, consumidores y empresas en línea y permitir una internet libre, **más segura** y legal.



### Enmienda 3

#### Propuesta de Reglamento Considerando 4 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

*(4 bis) El Centro de Competencia y sus acciones deben tener en cuenta la aplicación del Reglamento (UE) 2019/XXX [versión refundida del Reglamento (CE) n.º 428/2009 tal y como se propone en COM(2016)616]1 bis.*

---

*1 bis Reglamento (UE) 2019/... del Parlamento Europeo y del Consejo, de ..., por el que se establece un régimen de la Unión de control de las exportaciones, la transferencia, el corretaje, la asistencia técnica y el tránsito de productos de doble uso ( DO L ... de ..., p. ...).*

### Enmienda 4

#### Propuesta de Reglamento Considerando 8

*Texto de la Comisión*

*Enmienda*

(8) El Centro de Competencia ha de ser el principal instrumento de la Unión para poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad y ejecutar los proyectos e iniciativas pertinentes junto con la red de competencias en ciberseguridad. Debe prestar apoyo financiero en relación con la ciberseguridad a través de los programas Horizonte Europa y Europa Digital, y estar abierto al Fondo Europeo de Desarrollo Regional y a otros programas cuando proceda. Se espera que este enfoque contribuya a crear sinergias, coordinar el apoyo financiero relacionado con la

(8) El Centro de Competencia ha de ser el principal instrumento de la Unión para poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad y ejecutar los proyectos e iniciativas pertinentes junto con la red de competencias en ciberseguridad. Debe prestar apoyo financiero en relación con la ciberseguridad a través de los programas Horizonte Europa y Europa Digital, **así como del Fondo Europeo de Defensa por lo que respecta a las actividades y los costes administrativos en materia de defensa**, y estar abierto al Fondo Europeo de Desarrollo Regional y a otros programas

*investigación*, la innovación, la tecnología y el desarrollo industrial en materia de ciberseguridad, y evitar la duplicación.

cuando proceda. Se espera que este enfoque contribuya a crear sinergias, coordinar el apoyo financiero relacionado con *iniciativas de la Unión en el ámbito de la I+D*, la innovación, la tecnología y el desarrollo industrial en materia de ciberseguridad, y evitar la duplicación.

## Enmienda 5

### Propuesta de Reglamento Considerando 8 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

***(8 bis) A la vista del alcance de los desafíos en materia de ciberseguridad y las inversiones en capacidades y competencias en el ámbito de la ciberseguridad en otras partes del mundo, la Unión y sus Estados miembros deben intensificar el apoyo financiero a la investigación, el desarrollo y la implantación en este ámbito. Con objeto de alcanzar economías de escala y de conseguir un nivel de protección comparable en toda la Unión, los Estados miembros deben centrar su esfuerzo en un marco europeo invirtiendo a través del mecanismo del Centro de Competencia, cuando proceda.***

## Enmienda 6

### Propuesta de Reglamento Considerando 8 ter (nuevo)

*Texto de la Comisión*

*Enmienda*

***(8 ter) La «seguridad desde el diseño» como principio debe influir también en los procesos de normalización formales y no formales, en los que una práctica común de normalización no formal es la creación de ejecuciones de referencia, publicadas en licencias abiertas y libres. El diseño seguro, en particular cuando se***

*trata de ejecuciones de referencia, es fundamental para la fiabilidad y la resiliencia en su conjunto de las infraestructuras de red y sistemas de información de uso común, como internet.*

## Enmienda 7

### Propuesta de Reglamento Considerando 9

#### *Texto de la Comisión*

(9) Teniendo en cuenta que los objetivos de la presente iniciativa pueden alcanzarse mejor *si participan* todos los Estados miembros o el mayor número posible de Estados miembros, y como incentivo para su participación, solo aquellos que contribuyan financieramente a los costes administrativos y de funcionamiento del Centro de Competencia deben tener derecho de voto.

#### *Enmienda*

(9) Teniendo en cuenta que los objetivos de la presente iniciativa pueden alcanzarse mejor *con la aportación de* todos los Estados miembros o el mayor número posible de Estados miembros, y como incentivo para su participación, solo aquellos que contribuyan financieramente a los costes administrativos y de funcionamiento del Centro de Competencia deben tener derecho de voto.

## Enmienda 8

### Propuesta de Reglamento Considerando 12

#### *Texto de la Comisión*

(12) Los Estados miembros deben seleccionar los centros nacionales de coordinación. Además de la capacidad administrativa necesaria, los centros han de poseer o tener acceso directo a conocimientos tecnológicos especializados en materia de ciberseguridad, especialmente en ámbitos como la criptografía, los servicios de seguridad de TIC, la detección de intrusiones, la seguridad de los sistemas, la seguridad de las redes, la seguridad de los programas informáticos y las aplicaciones, o los aspectos humanos y sociales de la seguridad y la privacidad. También se

#### *Enmienda*

(12) Los Estados miembros deben seleccionar los centros nacionales de coordinación. Además de la capacidad administrativa necesaria, los centros han de poseer o tener acceso directo a conocimientos tecnológicos especializados en materia de ciberseguridad, especialmente en ámbitos como la criptografía, los servicios de seguridad de TIC, la detección de intrusiones, la seguridad de los sistemas, la seguridad de las redes, la seguridad de los programas informáticos y las aplicaciones, o los aspectos humanos, *éticos* y sociales de la seguridad y la privacidad. También se

requiere que tengan la capacidad de comprometerse y coordinarse eficazmente con la industria, el sector público, incluidas las autoridades designadas con arreglo a la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo<sup>23</sup>, y la comunidad investigadora.

---

<sup>23</sup> 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. 1).

requiere que tengan la capacidad de comprometerse y coordinarse eficazmente con la industria, el sector público, incluidas las autoridades designadas con arreglo a la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo<sup>23</sup>, y la comunidad investigadora. ***Por otra parte, debe concienciarse en mayor medida al gran público a través de los medios de comunicación adecuados de la importancia de la ciberseguridad.***

---

<sup>23</sup> 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. 1).

## Enmienda 9

### Propuesta de Reglamento Considerando 15

#### *Texto de la Comisión*

(15) El Centro de Competencia debe tener varias funciones clave. En primer lugar, el Centro de Competencia debe facilitar y ayudar a coordinar la labor de la red europea de competencias en ciberseguridad y apoyar a la Comunidad de Competencias en Ciberseguridad. El Centro ha de impulsar el programa tecnológico de ciberseguridad y facilitar el acceso a los conocimientos especializados reunidos en la Red y en la Comunidad de Competencias en Ciberseguridad. En segundo lugar, es preciso que ejecute las partes pertinentes de los programas Europa Digital y Horizonte Europa mediante la concesión de subvenciones, normalmente tras una convocatoria de propuestas competitiva. En tercer lugar, el Centro de Competencia debe facilitar la inversión conjunta por la Unión, los Estados

#### *Enmienda*

(15) El Centro de Competencia debe tener varias funciones clave. En primer lugar, el Centro de Competencia debe facilitar y ayudar a coordinar la labor de la red europea de competencias en ciberseguridad y apoyar a la Comunidad de Competencias en Ciberseguridad. El Centro ha de impulsar el programa tecnológico de ciberseguridad y facilitar el acceso a los conocimientos especializados reunidos en la Red y en la Comunidad de Competencias en Ciberseguridad. En segundo lugar, es preciso que ejecute las partes pertinentes de los programas Europa Digital y Horizonte Europa, ***así como del Fondo Europeo de Defensa***, mediante la concesión de subvenciones, normalmente tras una convocatoria de propuestas competitiva. En tercer lugar, el Centro de Competencia debe facilitar la inversión

miembros y/o la industria.

conjunta por la Unión, los Estados miembros y/o la industria.

## Enmienda 10

### Propuesta de Reglamento

#### Considerando 16

##### *Texto de la Comisión*

(16) El Centro de Competencia ha de estimular y respaldar la cooperación y la coordinación de las actividades de la Comunidad de Competencias en Ciberseguridad, en la que participará un grupo amplio, abierto y diverso de agentes del ámbito de la tecnología de ciberseguridad. Dicha comunidad debe contar, en particular, con entidades de investigación, industrias de la oferta, industrias de la demanda y el sector público. Es preciso que la Comunidad de Competencias en Ciberseguridad contribuya a las actividades y al plan de trabajo del Centro de Competencia y que se beneficie asimismo de las actividades de desarrollo comunitario del Centro de Competencia y de la Red; sin embargo, no debe recibir un trato privilegiado en lo que respecta a las convocatorias de propuestas o licitaciones.

##### *Enmienda*

(16) El Centro de Competencia ha de estimular y respaldar la cooperación y la coordinación de las actividades de la Comunidad de Competencias en Ciberseguridad, en la que participará un grupo amplio, abierto y diverso de agentes del ámbito de la tecnología de ciberseguridad. Dicha comunidad debe contar, en particular, con entidades de investigación, ***incluidas aquellas que se dedican a la ética en el ámbito de la ciberseguridad***, industrias de la oferta, industrias de la demanda y el sector público. Es preciso que la Comunidad de Competencias en Ciberseguridad contribuya a las actividades y al plan de trabajo del Centro de Competencia y que se beneficie asimismo de las actividades de desarrollo comunitario del Centro de Competencia y de la Red; sin embargo, no debe recibir un trato privilegiado en lo que respecta a las convocatorias de propuestas o licitaciones.

## Enmienda 11

### Propuesta de Reglamento

#### Considerando 17

##### *Texto de la Comisión*

(17) Para dar respuesta a las necesidades de las industrias de la demanda y de la oferta, la función del Centro de Competencia de proporcionar a las industrias conocimientos y asistencia técnica en materia de ciberseguridad ha de

##### *Enmienda*

(17) Para dar respuesta a las necesidades de las industrias de la demanda y de la oferta, la función del Centro de Competencia de proporcionar a las industrias conocimientos y asistencia técnica en materia de ciberseguridad ha de

referirse tanto a los productos y servicios de TIC como a todos los demás productos y soluciones industriales y tecnológicos en los que deba integrarse la ciberseguridad.

referirse tanto a los productos, **procesos** y servicios de TIC como a todos los demás productos y soluciones industriales y tecnológicos en los que deba integrarse la ciberseguridad.

### *Justificación*

*En el contexto de las industrias afines, todos los actores de la cadena de valor deben velar por la ciberseguridad de sus productos, procesos y servicios de una forma dinámica desde la fase más temprana del proceso de ingeniería.*

## **Enmienda 12**

### **Propuesta de Reglamento Considerando 17 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**(17 bis) El Centro de Competencia en Ciberseguridad debe contribuir a una amplia implantación de los productos y sistemas de ciberseguridad de última generación, en particular de aquellos que gozan de reconocimiento internacional.**

## **Enmienda 13**

### **Propuesta de Reglamento Considerando 18**

*Texto de la Comisión*

*Enmienda*

**(18) Mientras que el Centro de Competencia y la Red deben esforzarse por lograr sinergias entre los ámbitos civil y militar de la ciberseguridad, los proyectos financiados por el programa Horizonte Europa se ejecutarán de conformidad con el Reglamento XXX [Reglamento relativo a Horizonte Europa], que dispone que las actividades de investigación e innovación llevadas a cabo en el marco de Horizonte Europa se centrarán en las aplicaciones civiles.**

(18) Los proyectos financiados por el programa Horizonte Europa se ejecutarán de conformidad con el Reglamento XXX [Reglamento relativo a Horizonte Europa], que dispone que las actividades de investigación e innovación llevadas a cabo en el marco de Horizonte Europa se centrarán en las aplicaciones civiles.

## Enmienda 14

### Propuesta de Reglamento Considerando 20 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

**(20 bis)** *Teniendo en cuenta que la Unión ya dispone de otra agencia europea especializada en ciberseguridad, ENISA, el Consejo de Administración del Centro de Competencia debe velar por que, al objeto de generar sinergias, se consulten a esta todas las actividades relevantes del Centro.*

## Enmienda 15

### Propuesta de Reglamento Considerando 21

*Texto de la Comisión*

*Enmienda*

(21) Habida cuenta de sus respectivos conocimientos especializados en materia de ciberseguridad, procede que el Centro Común de Investigación de la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) desempeñen un papel activo en la Comunidad de Competencias en Ciberseguridad y en el Consejo Consultivo Industrial y Científico.

(21) Habida cuenta de sus respectivos conocimientos especializados en materia de ciberseguridad, procede que, ***a fin de garantizar sinergias***, el Centro Común de Investigación de la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) desempeñen un papel activo en la Comunidad de Competencias en Ciberseguridad y en el Consejo Consultivo Industrial y Científico.

## Enmienda 16

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

*Texto de la Comisión*

*Enmienda*

**(21 bis)** *Habida cuenta de sus competencias respectivas en materia de ciberseguridad, deben buscarse sinergias entre la Agencia de Seguridad de las Redes y de la Información de la Unión*

*Europea (ENISA) y el Centro de Competencia, teniendo en cuenta que ENISA debe seguir cumpliendo sus objetivos estratégicos, especialmente en el ámbito de la certificación de la ciberseguridad, tal como se establece en el «Reglamento de Ciberseguridad»<sup>1 bis</sup>, mientras que el Centro de Competencia debe actuar como órgano operativo en el ámbito de la ciberseguridad.*

---

*<sup>1 bis</sup> Propuesta de Reglamento 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 [2017/0225(COD)].*

## **Enmienda 17**

### **Propuesta de Reglamento Considerando 25**

#### *Texto de la Comisión*

(25) Para que el Centro de Competencia funcione correcta y eficazmente, la Comisión y los Estados miembros han de garantizar que las personas que se nombren como miembros del Consejo de Administración disponen 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.

#### *Enmienda*

(25) Para que el Centro de Competencia funcione correcta y eficazmente, la Comisión y los Estados miembros han de garantizar que las personas que se nombren como miembros del Consejo de Administración disponen 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. ***ENISA debe asimismo desempeñar de manera permanente un papel consultivo, sin derecho a voto, en el Consejo de Administración, y se le deben consultar todas las actividades relevantes del Centro.***



## Enmienda 18

### Propuesta de Reglamento Considerando 27

#### *Texto de la Comisión*

(27) El Centro de Competencia debe contar con un Consejo Consultivo Industrial y Científico 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 Consejo Consultivo Industrial y Científico ha de centrarse en las cuestiones que afecten a las partes interesadas y ponerlas en conocimiento del Consejo de Administración del Centro de Competencia. La composición del Consejo Consultivo Industrial y Científico y las funciones asignadas a este, como la de ser consultado respecto al plan de trabajo, deben garantizar una representación suficiente de las partes interesadas en la labor del Centro de Competencia.

#### *Enmienda*

(27) El Centro de Competencia debe contar con un Consejo Consultivo Industrial y Científico 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. ***Debe asimismo prestar asesoramiento independiente en materia de contratación pública e implantación al director ejecutivo y al Consejo de Administración.*** El Consejo Consultivo Industrial y Científico ha de centrarse en las cuestiones que afecten a las partes interesadas y ponerlas en conocimiento del Consejo de Administración del Centro de Competencia. La composición del Consejo Consultivo Industrial y Científico y las funciones asignadas a este, como la de ser consultado respecto al plan de trabajo, deben garantizar una representación suficiente de las partes interesadas en la labor del Centro de Competencia. ***Se le debe asignar a todas las partes interesadas del sector un mínimo de miembros, con especial hincapié en la representación de las pymes.***

## Enmienda 19

### Propuesta de Reglamento Considerando 29

#### *Texto de la Comisión*

(29) El Centro de Competencia ha de contar con normas para la prevención y ***gestión*** de los conflictos de intereses. El Centro de Competencia debe aplicar, asimismo, las correspondientes disposiciones de la Unión relativas al

#### *Enmienda*

(29) El Centro de Competencia ha de contar con normas para la prevención, ***detección y resolución de conflictos de intereses en relación con sus miembros, organismos y personal, así como con el Consejo de Administración, el Consejo***

acceso del público a los documentos, según se establece en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo<sup>24</sup>. El tratamiento de los datos personales por parte del Centro de Competencia se ajustará al Reglamento (UE) n.º XXX/2018 del Parlamento Europeo y del Consejo. El Centro de Competencia debe cumplir las disposiciones aplicables a las instituciones de la Unión, así como la legislación nacional en materia de tratamiento de la información, en particular la información delicada no clasificada y la información clasificada de la UE.

***Consultivo Industrial y Científico, y la Comunidad.*** Los ***Estados miembros deben velar por la prevención, detección y resolución de conflictos de intereses por lo que respecta a los centros nacionales de coordinación.*** El Centro de Competencia debe aplicar, asimismo, las correspondientes disposiciones de la Unión relativas al acceso del público a los documentos, según se establece en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo<sup>24</sup>. El tratamiento de los datos personales por parte del Centro de Competencia se ajustará al Reglamento (UE) n.º XXX/2018 del Parlamento Europeo y del Consejo. El Centro de Competencia debe cumplir las disposiciones aplicables a las instituciones de la Unión, así como la legislación nacional en materia de tratamiento de la información, en particular la información delicada no clasificada y la información clasificada de la UE.

---

<sup>24</sup> Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

---

<sup>24</sup> Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

## Enmienda 20

### Propuesta de Reglamento Considerando 31

#### *Texto de la Comisión*

(31) El Centro de Competencia debe funcionar de manera abierta y transparente, facilitando en el momento adecuado toda la información pertinente y promocionando sus actividades, en particular mediante actividades de información y difusión destinadas al público en general. Debe hacerse público el reglamento interno de los órganos del Centro de Competencia.

#### *Enmienda*

(31) El Centro de Competencia debe funcionar de manera abierta y transparente, facilitando información de manera exhaustiva y en el momento adecuado y promocionando sus actividades, incluido mediante actividades de información y difusión destinadas al público en general. ***Debe facilitar al público y a cualquier parte interesada una lista de los miembros***

*de la Comunidad de Competencias en Ciberseguridad y hacer públicas las declaraciones de intereses que presenten de conformidad con el artículo 42. Debe hacerse público el reglamento interno de los órganos del Centro de Competencia.*

## **Enmienda 21**

### **Propuesta de Reglamento Considerando 31 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(31 bis) Sería recomendable que tanto el Centro de Competencia como los centros nacionales de coordinación supervisarán las normas internacionales e hicieran un seguimiento de ellas en la medida de lo posible, a fin de promover la elaboración de buenas prácticas mundiales.*

## **Enmienda 22**

### **Propuesta de Reglamento Considerando 31 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(31 ter) Representar la diversidad del conjunto de la sociedad puede ser positivo para la Comunidad de Ciberseguridad europea, la cual debe alcanzar una representación equilibrada en lo que a sexos, diversidad étnica y discapacidad respecta.*

## **Enmienda 23**

### **Propuesta de Reglamento Considerando 33 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(33 bis) Deben delegarse en la*

*Comisión los poderes para adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea, por lo que respecta a la definición de los elementos de los acuerdos contractuales entre el Centro de Competencia y los centros nacionales de coordinación, así como a la especificación de los criterios para la evaluación y acreditación de las entidades en cuantos miembros de la Comunidad de Competencias en Ciberseguridad. 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 de 13 de abril de 2016 sobre la mejora de la legislación. 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.*

## **Enmienda 24**

### **Propuesta de Reglamento Artículo 1 – apartado 2**

#### *Texto de la Comisión*

2. El Centro de Competencia contribuirá a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX, y en particular las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], y del programa Horizonte Europa, establecido por el Reglamento n.º XXX, y en particular la sección 2.2.6

#### *Enmienda*

2. El Centro de Competencia contribuirá a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX, y en particular las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], del programa Horizonte Europa, establecido por el Reglamento n.º XXX, y en particular la sección 2.2.6

del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico].

del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico], **y del Fondo Europeo de Defensa, establecido por el Reglamento n.º XXX.**

## Enmienda 25

### Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 1

#### *Texto de la Comisión*

1) «ciberseguridad», la protección de las redes y sistemas de información, sus usuarios y **otras** personas **frente a** las ciberamenazas;

#### *Enmienda*

1) «ciberseguridad», **todas las actividades necesarias para** la protección de las redes y sistemas de información, sus usuarios y **las** personas **afectadas por** las ciberamenazas;

## Enmienda 26

### Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 2

#### *Texto de la Comisión*

2) «productos y soluciones de ciberseguridad», los productos, servicios o procesos de TIC destinados específicamente a proteger las redes y sistemas de información, así como a sus usuarios y a las personas afectadas, frente a las ciberamenazas;

#### *Enmienda*

*(No afecta a la versión española).*

## Enmienda 27

### Propuesta de Reglamento Artículo 2 – párrafo 1 – punto 3

#### *Texto de la Comisión*

3) «autoridad pública», cualquier Gobierno u otra administración pública,

#### *Enmienda*

3) «autoridad pública», cualquier Gobierno u otra administración pública,

incluidos los organismos públicos consultivos, a nivel nacional, regional o local, o cualquier persona física o jurídica que desempeñe funciones administrativas públicas con arreglo al Derecho nacional, incluidas funciones específicas;

incluidos los organismos públicos consultivos, a nivel nacional, regional o local, o cualquier persona física o jurídica que desempeñe funciones administrativas públicas con arreglo al Derecho *de la Unión* y nacional, incluidas funciones específicas;

## Enmienda 28

### Propuesta de Reglamento

#### Artículo 2 – párrafo 1 – punto 4

##### *Texto de la Comisión*

4) «Estado miembro *participante*», el Estado miembro que contribuye voluntariamente a sufragar los costes administrativos y de funcionamiento del Centro de Competencia.

##### *Enmienda*

4) «Estado miembro *contribuyente*», el Estado miembro que contribuye voluntariamente a sufragar los costes administrativos y de funcionamiento del Centro de Competencia.

## Enmienda 29

### Propuesta de Reglamento

#### Artículo 3 – apartado 1 – letra a

##### *Texto de la Comisión*

a) mantener y desarrollar las capacidades tecnológicas e industriales en materia de ciberseguridad necesarias para garantizar la protección de su mercado único digital;

##### *Enmienda*

a) mantener y desarrollar las *facultades y* capacidades tecnológicas, *académicas e investigativas, sociales, e* industriales en materia de ciberseguridad necesarias para garantizar la protección de su mercado único digital *e impulsarlo, así como para promover la autonomía digital de Europa;*

## Enmienda 30

### Propuesta de Reglamento

#### Artículo 3 – apartado 1 – letra b

##### *Texto de la Comisión*

b) aumentar la competitividad de la industria de ciberseguridad de la Unión y

##### *Enmienda*

b) aumentar la competitividad de la industria de ciberseguridad de la Unión

*convertir* la ciberseguridad en una ventaja competitiva para otras industrias de la Unión.

*fomentando la adopción de los productos y sistemas de ciberseguridad creados en la Unión de modo que la ciberseguridad se convierta en una ventaja competitiva para otras industrias de la Unión, dotándola de una base sólida y situándola como actor clave en la lucha contra los ciberataques;*

## **Enmienda 31**

### **Propuesta de Reglamento**

#### **Artículo 3 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*b bis) aumentar la resiliencia y la fiabilidad de la industria de ciberseguridad de la Unión, las infraestructuras de las redes y los sistemas de información e internet, así como de los equipos y programas informáticos de uso común en la Unión de modo que se afiance la confianza de los ciudadanos, los consumidores y las empresas en el mundo digital contribuyendo, en consecuencia, a los objetivos de la Estrategia para el Mercado Único Digital;*

## **Enmienda 32**

### **Propuesta de Reglamento**

#### **Artículo 3 – apartado 1 – letra b ter (nueva)**

*Texto de la Comisión*

*Enmienda*

*b ter) sensibilizar en cuanto a los riesgos en materia de ciberseguridad y las repercusiones y preocupaciones sociales y éticas asociadas en la Unión;*

## **Enmienda 33**

### **Propuesta de Reglamento**

#### **Artículo 3 – apartado 1 – letra b quater (nueva)**

***b quater) apoyar, facilitar y acelerar los procesos de normalización y certificación.***

## Enmienda 34

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 1

Texto de la Comisión

1. facilitar y ayudar a coordinar la labor de la Red de Centros Nacionales de Coordinación (en lo sucesivo, la «Red») a que se refiere el artículo 6 y de la Comunidad de Competencias en Ciberseguridad a que se refiere el artículo 8;

Enmienda

1. facilitar y ayudar a coordinar la labor de la Red de Centros Nacionales de Coordinación (en lo sucesivo, la «Red») a que se refiere el artículo 6 y de la Comunidad de Competencias en Ciberseguridad ***(en lo sucesivo, la «Comunidad»)*** a que se refiere el artículo 8;

## Enmienda 35

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 2

Texto de la Comisión

2. contribuir a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX<sup>26</sup>, y en particular de las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], y del programa Horizonte Europa, establecido por el Reglamento n.º XXX<sup>27</sup>, y en particular la sección 2.2.6 del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico];

Enmienda

2. contribuir a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX<sup>26</sup>, y en particular de las acciones relacionadas con el artículo 6 del Reglamento (UE) n.º XXX [programa Europa Digital], y del programa Horizonte Europa, establecido por el Reglamento n.º XXX<sup>27</sup>, y en particular la sección 2.2.6 del pilar II del anexo I de la Decisión n.º XXX, por la que se establece el Programa Específico por el que se ejecuta el Programa Marco de Investigación e Innovación «Horizonte Europa» [número de referencia del Programa Específico], ***así como del Fondo Europeo de Defensa, establecido por el Reglamento n.º XXX, y***



*de otros programas de la Unión cuando así lo prevean los actos jurídicos de la Unión;*

---

<sup>26</sup> [añadir título completo y referencia del DO]

---

<sup>26</sup> [añadir título completo y referencia del DO]

<sup>27</sup> [añadir título completo y referencia del DO]

<sup>27</sup> [añadir título completo y referencia del DO]

## Enmienda 36

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – parte introductoria

##### *Texto de la Comisión*

3. mejorar las capacidades, los conocimientos y las infraestructuras en materia de ciberseguridad al servicio de la industria, el sector público y la comunidad investigadora a través de lo siguiente:

##### *Enmienda*

3. mejorar ***la resiliencia, las competencias***, las capacidades, los conocimientos y las infraestructuras en materia de ciberseguridad al servicio de la ***sociedad, la*** industria, el sector público y la comunidad investigadora a través de lo siguiente, ***habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos***:

## Enmienda 37

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra a

##### *Texto de la Comisión*

a) ***habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos***, adquirir estas infraestructuras y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión, desde la industria, ***incluidas*** las pymes, hasta el sector público y la comunidad

##### *Enmienda*

a) adquirir estas infraestructuras y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición, ***de manera equitativa, abierta y transparente***, de una amplia gama de usuarios en toda la Unión, desde la industria, ***en particular*** las pymes, hasta el sector público y la comunidad científica e investigadora;

científica e investigadora;

### Enmienda 38

#### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra b

##### *Texto de la Comisión*

b) ***habida cuenta de las infraestructuras industriales y de investigación de vanguardia en relación con la ciberseguridad y los servicios conexos, proporcionar apoyo a otras entidades, incluido de tipo financiero,*** para adquirir estas infraestructuras y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión, ***desde*** la industria, ***incluidas*** las pymes, ***hasta el*** sector público y la comunidad científica e investigadora;

##### *Enmienda*

b) adquirir estas infraestructuras y servicios conexos, actualizarlos, explotarlos y ponerlos a disposición de una amplia gama de usuarios en toda la Unión ***procedentes tanto de*** la industria, ***en particular*** las pymes, ***como del*** sector público y la comunidad científica e investigadora;

### Enmienda 39

#### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra b bis (nueva)

##### *Texto de la Comisión*

##### *Enmienda*

***b bis) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes, las pymes, las microempresas y los especialistas del ámbito de la ciberseguridad, a proyectos de programas informáticos libres, gratuitos y de código abierto, utilizados habitualmente en infraestructuras, productos y procesos, y a proyectos de tecnología cívica;***

### Enmienda 40

#### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra b ter (nueva)

*b ter) ofrecer auditorías de la codificación de la seguridad en los programas informáticos y mejoras en los proyectos de programas libres, gratuitos y de código abierto, utilizados habitualmente en infraestructuras, productos y procesos;*

## Enmienda 41

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra c

Texto de la Comisión

Enmienda

c) **proporcionar** conocimientos y asistencia técnica en materia de ciberseguridad **a** la industria y **a** las autoridades públicas, en particular apoyando las medidas destinadas a facilitar el acceso a los conocimientos especializados disponibles en la Red y en la Comunidad de Competencias en Ciberseguridad;

c) **facilitar el intercambio de** conocimientos y asistencia técnica en materia de ciberseguridad, **en particular entre las pymes, la industria manufacturera, la sociedad civil, la industria y las autoridades públicas, y la comunidad académica e investigadora**, en particular apoyando las medidas destinadas a facilitar el acceso a los conocimientos especializados disponibles en la Red y en la Comunidad de Competencias en Ciberseguridad;

## Enmienda 42

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 3 – letra c bis (nueva)

Texto de la Comisión

Enmienda

**c bis) promover la «seguridad desde el diseño» como principio en el proceso de desarrollo, mantenimiento, explotación y actualización de infraestructuras, productos y servicios, en particular apostando por métodos vanguardistas de desarrollo seguro, ensayos de seguridad satisfactorios y auditorías de seguridad;**

## Enmienda 43

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 4 – parte introductoria

##### *Texto de la Comisión*

4. contribuir a una amplia implantación de productos y soluciones de ciberseguridad de última generación en **todos** los sectores de la economía a través de lo siguiente:

##### *Enmienda*

4. contribuir a una amplia implantación de productos y soluciones de ciberseguridad **sostenible** y de última generación en **toda la Unión y en** los **distintos** sectores de la economía a través de lo siguiente:

## Enmienda 44

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 4 – letra a

##### *Texto de la Comisión*

a) estimular la investigación y el desarrollo en materia de ciberseguridad y la asimilación de los productos y soluciones de ciberseguridad de la Unión por parte de las autoridades públicas y **las industrias usuarias**;

##### *Enmienda*

a) estimular la investigación y el desarrollo en materia de ciberseguridad y la asimilación de los productos y soluciones de ciberseguridad de la Unión, **también** por parte de las autoridades públicas y **la industria**;

## Enmienda 45

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 4 – letra a bis (nueva)

##### *Texto de la Comisión*

##### *Enmienda*

**a bis) apoyar la investigación en el ámbito de la ciberdelincuencia;**

## Enmienda 46

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 4 – letra b

##### *Texto de la Comisión*

b) ayudar a las autoridades públicas, a

##### *Enmienda*

b) ayudar a las autoridades públicas, a

las industrias de la demanda y a otros usuarios a adoptar e integrar *las últimas* soluciones de ciberseguridad;

las industrias de la demanda y a otros usuarios a adoptar e integrar *productos y vanguardistas de uso común*;

#### Enmienda 47

##### Propuesta de Reglamento

##### Artículo 4 – párrafo 1 – punto 4 – letra c

###### *Texto de la Comisión*

c) apoyar en particular a las autoridades públicas en la organización de sus contratos públicos o llevar a cabo la contratación de productos y soluciones de ciberseguridad de vanguardia en nombre de las autoridades públicas;

###### *Enmienda*

c) apoyar en particular a las autoridades públicas en la organización de sus contratos públicos o llevar a cabo la contratación de productos y soluciones de ciberseguridad de vanguardia en nombre de las autoridades públicas, *también mediante el apoyo a la contratación pública desde el punto de vista medioambiental, social e innovador, de conformidad con las Directivas 2014/24/UE y 2014/25/UE*;

#### Enmienda 48

##### Propuesta de Reglamento

##### Artículo 4 – párrafo 1 – punto 4 – letra d

###### *Texto de la Comisión*

d) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes y las pymes del ámbito de la ciberseguridad para que entren en contacto con mercados potenciales y atraigan inversiones;

###### *Enmienda*

d) proporcionar apoyo financiero y asistencia técnica a las empresas emergentes, *los especialistas* y las pymes del ámbito de la ciberseguridad para que entren en contacto con mercados potenciales *y oportunidades de implantación*, y atraigan inversiones;

#### Enmienda 49

##### Propuesta de Reglamento

##### Artículo 4 – párrafo 1 – punto 4 – letra d bis (nueva)

*d bis) impulsar la adopción de la certificación de la ciberseguridad en consonancia con el Reglamento de Ciberseguridad;*

## Enmienda 50

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 5 – parte introductoria

Texto de la Comisión

Enmienda

5. mejorar la comprensión de la ciberseguridad y contribuir a reducir el déficit de capacidades en la Unión en relación con la ciberseguridad a través de lo siguiente:

5. mejorar la comprensión de la ciberseguridad, *también por parte de los particulares, sensibilizar en cuanto a la importancia que reviste la ciberseguridad para prevenir y encarar amenazas*, contribuir a reducir el déficit de capacidades *reforzando el nivel de capacitación* en la Unión en relación con la ciberseguridad, *y crear una sólida base de cibercapacidades* a través de lo siguiente:

## Enmienda 51

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 5 – letra a

Texto de la Comisión

Enmienda

a) promover un mayor desarrollo de las capacidades en materia de ciberseguridad, *colaborando, cuando proceda*, con los órganos y organismos pertinentes de la *UE*, en particular *la ENISA*;

a) promover un mayor desarrollo de las capacidades *y competencias* en materia de ciberseguridad, *fomentar que el nivel habitual de conocimientos en materia de ciberseguridad sea elevado y contribuir a la resiliencia de los usuarios y las infraestructuras de la Unión en coordinación* con los órganos y organismos pertinentes de la *Unión*, en particular *ENISA, especialmente mediante el desarrollo de programas de formación y campañas de sensibilización*;

## Enmienda 52

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 6 – letra a

##### *Texto de la Comisión*

a) proporcionar apoyo financiero a los esfuerzos de investigación en materia de ciberseguridad sobre la base de un **programa** industrial, tecnológico y de investigación, de carácter estratégico, plurianual y común, sometido a una evaluación y mejora constantes;

##### *Enmienda*

a) proporcionar apoyo financiero a los esfuerzos de investigación en materia de ciberseguridad sobre la base de un **plan** industrial, tecnológico y de investigación, de carácter estratégico, plurianual y común, sometido a una evaluación y mejora constantes;

## Enmienda 53

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 6 – letra b

##### *Texto de la Comisión*

b) apoyar proyectos de investigación y demostración a gran escala relativos a las capacidades tecnológicas de ciberseguridad de próxima generación, en colaboración con la industria y la Red;

##### *Enmienda*

b) apoyar proyectos de investigación y demostración a gran escala relativos a las capacidades tecnológicas de ciberseguridad de próxima generación, en colaboración con la industria, la Red **y la Comunidad**;

## Enmienda 54

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 6 – letra c

##### *Texto de la Comisión*

c) apoyar la investigación y la innovación en aras de la normalización en el ámbito de la tecnología de ciberseguridad;

##### *Enmienda*

c) apoyar la investigación y la innovación en aras de la **mejora de la** normalización en el ámbito de la tecnología de ciberseguridad **mediante una estrecha cooperación, en particular con las organizaciones europeas de normalización**;

## Enmienda 55

### Propuesta de Reglamento

**Artículo 4 – párrafo 1 – punto 6 – letra c bis (nueva)**

*Texto de la Comisión*

*Enmienda*

***c bis) apoyar el desarrollo de productos y sistemas de ciberseguridad independientes en estrecha cooperación con la industria, la Red y la Comunidad;***

**Enmienda 56**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 6 – letra c ter (nueva)**

*Texto de la Comisión*

*Enmienda*

***c ter) obtener las herramientas y las tecnologías necesarias para encarar los riesgos siempre cambiantes en relación con la ciberseguridad;***

**Enmienda 57**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 7 – letra c**

*Texto de la Comisión*

*Enmienda*

c) reunir a las partes interesadas para fomentar las sinergias entre la investigación y los mercados civil y militar de la ciberseguridad;

c) reunir a las partes interesadas para fomentar las sinergias entre la investigación y los mercados civil y militar de la ciberseguridad, ***armonizando las actividades, cuando proceda, con los órganos y organismos pertinentes de la Unión, en particular ENISA;***

**Enmienda 58**

**Propuesta de Reglamento**

**Artículo 4 – párrafo 1 – punto 8 – letra a**

*Texto de la Comisión*

*Enmienda*

a) ***proporcionar asesoramiento,*** compartir conocimientos especializados y facilitar la colaboración entre las partes

a) ***asesorar,*** compartir conocimientos especializados y facilitar la colaboración



interesadas pertinentes;

entre las partes interesadas pertinentes;

## Enmienda 59

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 8 – letra b

##### *Texto de la Comisión*

b) gestionar proyectos multinacionales de ciberdefensa, cuando así lo soliciten los Estados miembros, y de este modo ejercer de gestor de proyectos en el sentido del Reglamento XXX [Reglamento por el que se establece el Fondo Europeo de Defensa].

##### *Enmienda*

b) gestionar proyectos multinacionales **y transfronterizos** de ciberdefensa, cuando así lo soliciten los Estados miembros, y de este modo ejercer de gestor de proyectos en el sentido del Reglamento XXX [Reglamento por el que se establece el Fondo Europeo de Defensa];

## Enmienda 60

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 8 – letra b bis (nueva)

##### *Texto de la Comisión*

##### *Enmienda*

***b bis) contribuir, cuando proceda, a la evaluación tanto en relación con los derechos fundamentales como ética de las investigaciones en materia de ciberseguridad financiadas por el Centro de Competencia;***

## Enmienda 61

### Propuesta de Reglamento

#### Artículo 4 – párrafo 1 – punto 8 bis (nuevo)

##### *Texto de la Comisión*

##### *Enmienda*

***8 bis. contribuir a los esfuerzos de la Unión por reforzar la cooperación en materia de ciberseguridad a través de lo siguiente:***

***a) impulsar la participación de la Red y la Comunidad en conferencias internacionales;***

**b) cooperar con terceros países y organizaciones internacionales dentro de los marcos de cooperación internacional pertinentes.**

## **Enmienda 62**

### **Propuesta de Reglamento Artículo 6 – apartado 5**

#### *Texto de la Comisión*

5. La relación entre el Centro de Competencia y los centros nacionales de coordinación se basará en un acuerdo contractual firmado entre el Centro de Competencia y cada uno de los centros nacionales de coordinación. El acuerdo **establecerá** las normas por las que se regirán las relaciones y el reparto de funciones entre el Centro de Competencia y cada centro nacional de coordinación.

#### *Enmienda*

5. La relación entre el Centro de Competencia y los centros nacionales de coordinación se basará en un acuerdo contractual firmado entre el Centro de Competencia y cada uno de los centros nacionales de coordinación. El acuerdo **consistirá en el mismo conjunto de condiciones generales que establezca** las normas por las que se regirán las relaciones y el reparto de funciones entre el Centro de Competencia y cada centro nacional de coordinación **y las condiciones especiales adaptadas al centro nacional de coordinación de que se trate.**

## **Enmienda 63**

### **Propuesta de Reglamento Artículo 6 – apartado 5 bis (nuevo)**

#### *Texto de la Comisión*

#### *Enmienda*

**5 bis. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo -45 por los que se definan los elementos de los acuerdos contractuales a que se refiere el apartado 5 del presente artículo, en particular su formato.**

## **Enmienda 64**

### **Propuesta de Reglamento Artículo 7 – apartado 1 – letra a**

*Texto de la Comisión*

a) apoyar al Centro de Competencia en pos de la consecución de sus objetivos, y en particular en lo referente **a** la coordinación de la Comunidad de Competencias en Ciberseguridad;

*Enmienda*

a) apoyar al Centro de Competencia en pos de la consecución de sus objetivos, y en particular en lo referente **al establecimiento** y la coordinación de la Comunidad de Competencias en Ciberseguridad;

**Enmienda 65**

**Propuesta de Reglamento**

**Artículo 7 – apartado 1 – letra b**

*Texto de la Comisión*

b) **facilitar** la participación de la industria y de otros agentes a nivel de los Estados miembros en proyectos transfronterizos;

*Enmienda*

b) **promover, fomentar y facilitar** la participación de la **sociedad civil, de las organizaciones de consumidores, de los profesionales de la universidad e investigadores, de la industria, en especial las empresas emergentes y las pymes**, y de otros agentes a nivel de los Estados miembros en proyectos transfronterizos;

**Enmienda 66**

**Propuesta de Reglamento**

**Artículo 7 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

**b bis) incentivar los proyectos transfronterizos, en particular para las pymes;**

**Enmienda 67**

**Propuesta de Reglamento**

**Artículo 7 – apartado 1 – letra c**

*Texto de la Comisión*

c) contribuir, junto con el Centro de Competencia, a identificar y hacer frente a

*Enmienda*

c) contribuir, junto con el Centro de Competencia, a identificar y hacer frente a

los retos *industriales* en materia de ciberseguridad específicos de cada sector;

los retos en materia de ciberseguridad específicos de cada sector, *en particular el ciberespionaje*;

## Enmienda 68

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra c bis (nueva)

*Texto de la Comisión*

*Enmienda*

*c bis) cooperar estrechamente con las organizaciones nacionales de normalización para garantizar la asimilación de las normas en vigor y buscar la participación de todas las partes interesadas pertinentes, sobre todo las pymes, en la definición de nuevas normas;*

## Enmienda 69

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra e

*Texto de la Comisión*

*Enmienda*

e) tratar de establecer sinergias con las actividades oportunas a nivel nacional y regional;

e) tratar de establecer sinergias con las actividades oportunas a nivel nacional, regional *y local al objeto de que la Unión sea segura*;

## Enmienda 70

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra f bis (nueva)

*Texto de la Comisión*

*Enmienda*

*f bis) promover y difundir un plan de estudios mínimo sobre ciberseguridad en cooperación con los órganos oportunos de los Estados miembros;*

## Enmienda 71

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra g

##### *Texto de la Comisión*

g) promover y difundir los resultados pertinentes de la labor de la Red, la Comunidad de Competencias en Ciberseguridad y el Centro de Competencia a nivel nacional *o* regional;

##### *Enmienda*

g) promover y difundir los resultados pertinentes de la labor de la Red, la Comunidad de Competencias en Ciberseguridad y el Centro de Competencia a nivel nacional, regional y *local*;

## Enmienda 72

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra h

##### *Texto de la Comisión*

h) evaluar las solicitudes de las entidades *establecidas* en el mismo Estado miembro que el centro de coordinación para formar parte de la Comunidad de Competencias en Ciberseguridad.

##### *Enmienda*

h) evaluar las solicitudes de las entidades *y los particulares establecidos* en el mismo Estado miembro que el centro de coordinación para formar parte de la Comunidad de Competencias en Ciberseguridad;

## Enmienda 73

### Propuesta de Reglamento

#### Artículo 7 – apartado 1 – letra h bis (nueva)

##### *Texto de la Comisión*

##### *Enmienda*

*h bis) impulsar campañas de sensibilización, en particular dirigidas a las pymes, y facilitar, junto con el Centro de Competencia, las capacidades y los sistemas necesarios en materia de ciberseguridad.*

## Enmienda 74

### Propuesta de Reglamento

#### Artículo 8 – apartado 1

*Texto de la Comisión*

1. La Comunidad de Competencias en Ciberseguridad contribuirá a la misión del Centro de Competencia, según se establece en el artículo 3, y reforzará y difundirá los conocimientos especializados en materia de ciberseguridad en toda la Unión.

*Enmienda*

1. La Comunidad de Competencias en Ciberseguridad contribuirá a la misión del Centro de Competencia, según se establece en el artículo 3, reforzará y difundirá los conocimientos especializados en materia de ciberseguridad en toda la Unión, y **proporcionará asesoramiento técnico.**

**Enmienda 75**

**Propuesta de Reglamento**

**Artículo 8 – apartado 2**

*Texto de la Comisión*

2. La Comunidad de Competencias en Ciberseguridad estará compuesta por la industria, organizaciones de investigación del ámbito universitario y sin ánimo de lucro, asociaciones y entidades públicas y otras entidades que se ocupen de cuestiones operativas y técnicas. Reunirá a las principales partes interesadas en relación con las capacidades tecnológicas e industriales en materia de ciberseguridad de la Unión. Contará con la participación de los centros nacionales de coordinación, así como las instituciones y los organismos de la Unión que dispongan de los conocimientos especializados pertinentes.

*Enmienda*

2. La Comunidad de Competencias en Ciberseguridad estará compuesta por la **sociedad civil**, industria, **pymes incluidas, organizaciones europeas de normalización, asociaciones de usuarios, organizaciones de investigación del ámbito universitario y sin ánimo de lucro, asociaciones activas a escala nacional o europea**, y entidades públicas y otras entidades **o particulares** que se ocupen de cuestiones operativas y técnicas. Reunirá a las principales partes interesadas en relación con las capacidades **y facultades** tecnológicas e industriales, **sociales, y académicas e investigativas** en materia de ciberseguridad de la Unión. Contará con la participación de los centros nacionales de coordinación, así como las instituciones y los organismos de la Unión que dispongan de los conocimientos especializados pertinentes.

**Enmienda 76**

**Propuesta de Reglamento**

**Artículo 8 – apartado 3 bis (nuevo)**

**3 bis. La totalidad de las infraestructuras, instalaciones, activos y recursos financiados por el Centro de Competencia estarán situados en el territorio de los Estados miembros.**

## Enmienda 77

### Propuesta de Reglamento Artículo 8 – apartado 4

Texto de la Comisión

4. El Centro de Competencia acreditará a las entidades **establecidas con arreglo a la legislación nacional** como miembros de la Comunidad de Competencias en Ciberseguridad, previa evaluación realizada por el centro nacional de coordinación del Estado miembro en el que esté establecida la entidad acerca del cumplimiento de los criterios establecidos en el apartado 3 por parte de dicha entidad. La acreditación no tendrá una duración limitada, pero podrá ser revocada por el Centro de Competencia en cualquier momento si este o el centro nacional de coordinación pertinente considera que la entidad no cumple los criterios establecidos en el apartado 3 o entra en el ámbito de aplicación de las correspondientes disposiciones del artículo 136 del Reglamento XXX [nuevo Reglamento Financiero].

Enmienda

4. El Centro de Competencia acreditará a las entidades **sobre la base del apartado 3** como miembros de la Comunidad de Competencias en Ciberseguridad, previa evaluación realizada por el centro nacional de coordinación del Estado miembro en el que esté establecida la entidad acerca del cumplimiento de los criterios establecidos en el apartado 3 por parte de dicha entidad. La acreditación no tendrá una duración limitada, pero podrá ser revocada por el Centro de Competencia en cualquier momento si este o el centro nacional de coordinación pertinente considera que la entidad no cumple los criterios establecidos en el apartado 3 o entra en el ámbito de aplicación de las correspondientes disposiciones del artículo 136 del Reglamento XXX [nuevo Reglamento Financiero].

## Enmienda 78

### Propuesta de Reglamento Artículo 8 – apartado 4 bis (nuevo)

Texto de la Comisión

Enmienda

**4 bis. Los centros nacionales de coordinación de los Estados miembros**

*aspirarán a lograr en la Comunidad una representación equilibrada de las partes interesadas, en particular las pymes, y fomentará de manera activa la participación de aquellas categorías de partes interesadas que estén infrarrepresentadas.*

## **Enmienda 79**

### **Propuesta de Reglamento Artículo 8 – apartado 4 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

*4 ter. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo -45 por los que se especifiquen con mayor precisión los criterios previstos en el apartado 3 y los procedimientos para evaluar y acreditar a las entidades que cumplan dichos criterios.*

## **Enmienda 80**

### **Propuesta de Reglamento Artículo 9 – párrafo 1 – punto 5 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*5 bis) animarán a los miembros de la Comunidad que sean fabricantes y proveedores de servicios a que certifiquen sus productos y servicios conforme a los sistemas de certificación aprobados en virtud del Reglamento de Ciberseguridad.*

## **Enmienda 81**

### **Propuesta de Reglamento Artículo 10 – apartado 2**

*Texto de la Comisión*

*Enmienda*

2. La cooperación se llevará a cabo en el marco de convenios de trabajo. Estos

2. La cooperación se llevará a cabo en el marco de convenios de trabajo



convenios *se someterán a* la aprobación previa de la Comisión.

*acordados entre el Centro de Competencia y la institución, órgano u organismo correspondiente de la Unión.* Estos convenios *serán adoptados por el Consejo de Administración tras haber recibido* la aprobación previa de la Comisión.

## Enmienda 82

### Propuesta de Reglamento Artículo 12 – apartado 1

#### *Texto de la Comisión*

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y cinco representantes de la Comisión, en nombre de la Unión.

#### *Enmienda*

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y cinco representantes de la Comisión, en nombre de la Unión. ***El Consejo de Administración incluirá también a un miembro nombrado por el Parlamento Europeo, sin derecho a voto.***

## Enmienda 83

### Propuesta de Reglamento Artículo 12 – apartado 3

#### *Texto de la Comisión*

3. Los miembros del Consejo de Administración y sus suplentes serán nombrados en función de sus conocimientos en el ámbito ***tecnológico***, así como las correspondientes capacidades en materia de presupuestos, administración y gestión. La Comisión y los Estados miembros procurarán limitar la rotación de sus representantes en el Consejo de Administración con el fin de garantizar la continuidad en la labor de este órgano. La Comisión y los Estados miembros ***tratarán de lograr*** una representación equilibrada entre hombres y mujeres en el Consejo de Administración.

#### *Enmienda*

3. Los miembros del Consejo de Administración y sus suplentes serán nombrados en función de sus conocimientos en el ámbito ***de la tecnología o la investigación en materia de ciberseguridad***, así como las correspondientes capacidades en materia de presupuestos, administración y gestión. La Comisión y los Estados miembros procurarán limitar la rotación de sus representantes en el Consejo de Administración con el fin de garantizar la continuidad en la labor de este órgano. La Comisión y los Estados miembros ***velarán por*** una representación equilibrada entre hombres y mujeres en el Consejo de

## Enmienda 84

### Propuesta de Reglamento Artículo 12 – apartado 6

#### *Texto de la Comisión*

6. **La Comisión** podrá invitar observadores, incluidos representantes de **los** órganos y organismos de la Unión pertinentes, para que participen en las reuniones del Consejo de Administración, cuando proceda.

#### *Enmienda*

6. **El Consejo de Administración** podrá invitar observadores, incluidos representantes **del Consejo Consultivo Industrial y Científico** y de **otros** órganos y organismos de la Unión pertinentes, para que participen en las reuniones del Consejo de Administración, cuando proceda, **a fin de garantizar la incorporación de conocimientos especializados y de crear vínculos más sólidos con las comunidades industrial y de investigación.**

## Enmienda 85

### Propuesta de Reglamento Artículo 12 – apartado 7 bis (nuevo)

#### *Texto de la Comisión*

#### *Enmienda*

**7 bis. El presidente del Consejo Consultivo Industrial y Científico podrá asistir en calidad de observador sin derecho de voto a las reuniones del Consejo de Administración cuando en estas se aborden cuestiones relacionadas con las funciones de dicho Consejo en virtud del artículo 20.**

## Enmienda 86

### Propuesta de Reglamento Artículo 16 – apartado 1

#### *Texto de la Comisión*

#### *Enmienda*

1. El director ejecutivo será una persona con **conocimientos especializados**

1. El director ejecutivo será una persona con **un exhaustivo conocimiento**

*y una gran reputación* en los ámbitos en los que actúe el Centro de Competencia.

*especializado y experiencia profesional* en los ámbitos en los que actúe el Centro de Competencia.

## **Enmienda 87**

### **Propuesta de Reglamento Artículo 16 – apartado 3**

#### *Texto de la Comisión*

3. El Consejo de Administración nombrará al director ejecutivo a partir de una lista de candidatos propuesta por la Comisión después de un procedimiento de selección abierto y transparente.

#### *Enmienda*

3. El Consejo de Administración nombrará al director ejecutivo a partir de una lista de candidatos propuesta por la Comisión después de un procedimiento de selección abierto, transparente y *no discriminatorio dentro del respeto a la igualdad de género*.

## **Enmienda 88**

### **Propuesta de Reglamento Artículo 16 – apartado 5**

#### *Texto de la Comisión*

5. El mandato del director ejecutivo tendrá una duración de *cuatro* años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las tareas y los desafíos futuros del Centro de Competencia.

#### *Enmienda*

5. El mandato del director ejecutivo tendrá una duración de *cinco* años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las tareas y los desafíos futuros del Centro de Competencia.

## **Enmienda 89**

### **Propuesta de Reglamento Artículo 16 – apartado 6**

#### *Texto de la Comisión*

6. A propuesta de la Comisión, que tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá ampliar una vez el mandato del director ejecutivo, por un

#### *Enmienda*

6. A propuesta de la Comisión, que tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá ampliar una vez el mandato del director ejecutivo, por un

plazo máximo de *cuatro* años.

plazo máximo de *cinco* años.

## Enmienda 90

### Propuesta de Reglamento

#### Artículo 17 – apartado 2 – letra h

##### *Texto de la Comisión*

h) elaborar un plan de actuación sobre la base de las conclusiones de las evaluaciones retrospectivas e informar a la Comisión cada dos años de los progresos al respecto;

##### *Enmienda*

h) elaborar un plan de actuación sobre la base de las conclusiones de las evaluaciones retrospectivas e informar ***al Parlamento Europeo y*** a la Comisión cada dos años de los progresos al respecto;

## Enmienda 91

### Propuesta de Reglamento

#### Artículo 17 – apartado 2 – letra s

##### *Texto de la Comisión*

s) elaborar un plan de actuación sobre la base de las conclusiones de los informes de las auditorías internas o externas, así como de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF), y presentar informes sobre los progresos realizados, dos veces al año a la Comisión y periódicamente al Consejo de Administración;

##### *Enmienda*

s) elaborar un plan de actuación sobre la base de las conclusiones de los informes de las auditorías internas o externas, así como de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF), y presentar informes sobre los progresos realizados, dos veces al año ***al Parlamento Europeo y*** a la Comisión y periódicamente al Consejo de Administración;

## Enmienda 92

### Propuesta de Reglamento

#### Artículo 18 – apartado 1

##### *Texto de la Comisión*

1. El Consejo Consultivo Industrial y Científico tendrá un máximo de ***dieciséis*** miembros. Los miembros serán nombrados por el Consejo de Administración de entre los representantes de las entidades de la Comunidad de Competencias en

##### *Enmienda*

1. El Consejo Consultivo Industrial y Científico tendrá un máximo de ***veinticinco*** miembros. Los miembros serán nombrados por el Consejo de Administración de entre los representantes de las entidades de la Comunidad de Competencias en

Ciberseguridad.

Ciberseguridad *con arreglo a un procedimiento abierto, transparente y no discriminatorio.*

### Enmienda 93

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

*Texto de la Comisión*

*Enmienda*

***1 bis. La composición del Consejo Consultivo Industrial y Científico será equilibrada, contando con una adecuada representación de la industria, en particular las pymes, el mundo académico y la sociedad civil, incluidas las organizaciones de consumidores.***

### Enmienda 94

#### Propuesta de Reglamento Artículo 18 – apartado 2

*Texto de la Comisión*

*Enmienda*

2. Los miembros del Consejo Consultivo Industrial y Científico tendrán conocimientos especializados en materia de ***investigación sobre*** ciberseguridad, ***desarrollo industrial, servicios profesionales o implantación de servicios profesionales. El Consejo de Administración especificará con más detalle los requisitos acerca de dichos conocimientos especializados.***

2. Los miembros del Consejo Consultivo Industrial y Científico tendrán conocimientos especializados en materia de ciberseguridad ***en al menos uno*** de los ***ámbitos siguientes:***

- a) investigación;***
- b) desarrollo industrial;***
- c) formación y educación.***

### Enmienda 95

#### Propuesta de Reglamento Artículo 18 – apartado 4

*Texto de la Comisión*

4. El mandato de los miembros del Consejo Consultivo Industrial y Científico tendrá una duración de **tres** años. Este mandato será renovable.

*Enmienda*

4. El mandato de los miembros del Consejo Consultivo Industrial y Científico tendrá una duración de **cuatro** años. Este mandato será renovable.

**Enmienda 96**

**Propuesta de Reglamento  
Artículo 18 – apartado 5**

*Texto de la Comisión*

5. Los representantes de la Comisión y de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea **podrán apoyar y participar en** la labor del Consejo Consultivo Industrial y Científico.

*Enmienda*

5. Los representantes de la Comisión y de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea **apoyarán** la labor del Consejo Consultivo Industrial y Científico **y participarán en ella.**

**Enmienda 97**

**Propuesta de Reglamento  
Artículo 19 – apartado 1**

*Texto de la Comisión*

1. El Consejo Consultivo Industrial y Científico se reunirá como mínimo **dos** veces al año.

*Enmienda*

1. El Consejo Consultivo Industrial y Científico se reunirá como mínimo **tres** veces al año.

**Enmienda 98**

**Propuesta de Reglamento  
Artículo 20 – párrafo 1 – punto 1 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**1 bis) asesorar al Consejo de Administración acerca de la creación de grupos de trabajo, bajo la coordinación general de uno o varios miembros del Consejo Consultivo Industrial y Científico, sobre cuestiones específicas de**

*interés en relación con la labor del Centro de Competencia, para lo que nombrará a los participantes en dichos grupos;*

## **Enmienda 99**

### **Propuesta de Reglamento**

#### **Artículo 20 – párrafo 1 – punto 1 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

*1 ter) proporcionar al director ejecutivo y al Consejo de Administración un proyecto de programa de I+D a medio y largo plazo sobre la tecnología de ciberseguridad;*

## **Enmienda 100**

### **Propuesta de Reglamento**

#### **Artículo 20 – párrafo 1 – punto 3 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*3 bis) impulsar la cooperación sobre la base de iniciativas pasadas y presentes de la Unión entre diversas partes interesadas en el ámbito de la ciberseguridad.*

## **Enmienda 101**

### **Propuesta de Reglamento**

#### **Artículo 21 – apartado 1 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

*b bis) un importe del Fondo Europeo de Defensa para las actividades y los costes administrativos en materia de defensa.*

## **Enmienda 102**

### **Propuesta de Reglamento**

#### **Artículo 21 – apartado 4**

*Texto de la Comisión*

4. **La contribución financiera de la Unión no** cubrirá las funciones mencionadas en el artículo 4, apartado 8, letra b).

*Enmienda*

4. **El Fondo Europeo de Defensa** cubrirá las funciones mencionadas en el artículo 4, apartado 8, letra b).

**Enmienda 103**

**Propuesta de Reglamento  
Artículo 22 – apartado 4**

*Texto de la Comisión*

4. **La Comisión podrá poner fin, reducir proporcionalmente o suspender la contribución financiera de la Unión al Centro de Competencia en caso de que los Estados miembros participantes no aporten, aporten solo parcialmente o aporten con retraso las contribuciones a que se refiere el apartado 1.**

*Enmienda*

**suprimido**

**Enmienda 104**

**Propuesta de Reglamento  
Artículo 23 – apartado 8 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**8 bis. El Centro de Competencia cooperará estrechamente con otras instituciones y agencias de la Unión, en particular ENISA y otros órganos oportunos.**

**Enmienda 105**

**Propuesta de Reglamento  
Artículo 35 – apartado 2**

*Texto de la Comisión*

2. El Centro de Competencia velará por que **el** público y las partes interesadas

*Enmienda*

2. El Centro de Competencia velará por que **se facilite al** público y **a** las partes



*reciban* información *adecuada*, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de *su* labor. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 41.

interesadas información *completa*, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de *la* labor *del Centro de Competencia, la Red, el Consejo Consultivo Industrial y Científico y la Comunidad*. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 42.

#### *Justificación*

*Se ha corregido la referencia «artículo 41» por «artículo 42», tal como se acordó con la Comisión.*

### **Enmienda 106**

#### **Propuesta de Reglamento Artículo 35 – apartado 2 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**2 bis. El Centro de Competencia facilitará al público y a cualquier parte interesada una lista de los miembros de la Comunidad de Competencias en Ciberseguridad y hará públicas las declaraciones de intereses que presenten de conformidad con el artículo 42.**

### **Enmienda 107**

#### **Propuesta de Reglamento Artículo 38 – apartado 3**

*Texto de la Comisión*

*Enmienda*

3. La evaluación a que se refiere el apartado 2 incluirá un balance de los resultados alcanzados por el Centro de Competencia, a la vista de sus objetivos, su mandato y sus funciones. Si la Comisión considera que la continuidad del Centro de Competencia está justificada con respecto a los objetivos, el mandato y las funciones que le han sido asignados, podrá proponer

3. La evaluación a que se refiere el apartado 2 incluirá un balance de los resultados alcanzados por el Centro de Competencia, a la vista de sus objetivos, su mandato y sus funciones, **así como otro balance de la eficacia y la eficiencia del Centro de Competencia en la consecución de dichos resultados**. Si la Comisión considera que la continuidad del Centro de

que se amplíe la duración del mandato del Centro de Competencia establecida en el artículo 46.

Competencia está justificada con respecto a los objetivos, el mandato y las funciones que le han sido asignados, podrá proponer que se amplíe la duración del mandato del Centro de Competencia establecida en el artículo 46.

## Enmienda 108

### Propuesta de Reglamento Artículo 42 – párrafo 1

#### *Texto de la Comisión*

El Consejo de Administración del Centro de Competencia adoptará normas para la prevención y gestión de los conflictos de intereses en relación con sus miembros, sus órganos o su personal. Dichas normas contendrán disposiciones destinadas a evitar los conflictos de intereses en relación con los representantes de los miembros que formen parte del Consejo de Administración, así como el Consejo Consultivo Industrial y Científico, de conformidad con el Reglamento XXX [nuevo Reglamento Financiero].

#### *Enmienda*

El Consejo de Administración del Centro de Competencia adoptará normas para la prevención y gestión de los conflictos de intereses en relación con sus miembros, sus órganos o su personal, ***incluido el director ejecutivo***. Dichas normas contendrán disposiciones destinadas a evitar los conflictos de intereses en relación con los representantes de los miembros que formen parte del Consejo de Administración, así como el Consejo Consultivo Industrial y Científico, de conformidad con el Reglamento XXX [nuevo Reglamento Financiero].

## Enmienda 109

### Propuesta de Reglamento Artículo 42 – párrafo 1 bis (nuevo)

#### *Texto de la Comisión*

#### *Enmienda*

***Los Estados miembros velarán por la prevención, detección y resolución de conflictos de intereses por lo que respecta a los centros nacionales de coordinación.***

## Enmienda 110

### Propuesta de Reglamento Artículo 44 – párrafo -1 (nuevo)

***El Estado miembro anfitrión ofrecerá las mejores condiciones posibles para garantizar el buen funcionamiento del Centro de Competencia, lo que incluye una sede única, 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 parejas.***

## **Enmienda 111**

### **Propuesta de Reglamento Artículo 44 – párrafo 1**

*Texto de la Comisión*

***Podrá celebrarse*** un convenio administrativo entre el Centro de Competencia y el Estado miembro [Bélgica] en el que esté establecida su sede en relación con los privilegios e inmunidades y otro tipo de apoyo que deba conceder dicho Estado miembro al Centro de Competencia.

*Enmienda*

***Se celebrará*** un convenio administrativo entre el Centro de Competencia y el Estado miembro [Bélgica] en el que esté establecida su sede en relación con los privilegios e inmunidades y otro tipo de apoyo que deba conceder dicho Estado miembro al Centro de Competencia.

## **Enmienda 112**

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

*Texto de la Comisión*

*Enmienda*

#### ***Artículo 44 bis***

##### ***Ejercicio de la delegación***

- 1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.***
- 2. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 5 bis, y el artículo 8, apartado 4 ter, se otorgan a la Comisión por un***

*período de tiempo indefinido a partir del ... [fecha de entrada en vigor del presente Reglamento].*

**3. La delegación de poderes mencionada en el artículo 6, apartado 5 bis, y el artículo 8, apartado 4 ter, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.**

**4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.**

**5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.**

**6. Los actos delegados adoptados en virtud del artículo 6, apartado 5 bis, y del artículo 8, apartado 4 ter, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.**

*(Este artículo forma parte del capítulo VII).*

## PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

<b>Título</b>	Establecimiento del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación	
<b>Referencias</b>	COM(2018)0630 – C8-0404/2018 – 2018/0328(COD)	
<b>Comisiones competentes para el fondo</b> Fecha del anuncio en el Pleno	ITRE 1.10.2018	
<b>Opinión emitida por</b> Fecha del anuncio en el Pleno	IMCO 1.10.2018	
<b>Ponente de opinión</b> Fecha de designación	Arndt Kohn 24.9.2018	
<b>Examen en comisión</b>	6.12.2018	21.1.2019
<b>Fecha de aprobación</b>	29.1.2019	
<b>Resultado de la votación final</b>	+: 31 -: 2 0: 0	
<b>Miembros presentes en la votación final</b>	Pascal Arimont, Carlos Coelho, Sergio Gaetano Cofferati, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Pascal Durand, Evelyne Gebhardt, Maria Grapini, Liisa Jaakonsaari, Philippe Juvin, Nosheena Mobarik, Jiří Pospíšil, Marcus Pretzell, Virginie Rozière, Christel Schaldemose, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Igor Šoltes, Ivan Štefanec, Róza Gräfin von Thun und Hohenstein, Mihai Țurcanu, Anneleen Van Bossuyt, Marco Zullo	
<b>Suplentes presentes en la votación final</b>	Biljana Borzan, Nadja Hirsch, Arndt Kohn, Adam Szejnfeld, Marc Tarabella, Matthijs van Miltenburg, Lambert van Nistelrooij	
<b>Suplentes (art. 200, apdo. 2) presentes en la votación final</b>	John Stuart Agnew	

**VOTACIÓN FINAL NOMINAL  
EN LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN**

<b>31</b>	<b>+</b>
ALDE	Nadja Hirsch, Matthijs van Miltenburg, Jasenko Selimovic
ECR	Daniel Dalton, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Philippe Juvin, Lambert van Nistelrooij, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Róza Gräfin von Thun und Hohenstein, Mihai Țurcanu
S&D	Biljana Borzan, Sergio Gaetano Cofferati, Nicola Danti, Evelyne Gebhardt, Maria Grapini, Liisa Jaakonsaari, Arndt Kohn, Virginie Rozière, Christel Schaldemose, Olga Sehnalová, Marc Tarabella
Verts/ALE	Pascal Durand, Igor Šoltes

<b>2</b>	<b>-</b>
ENF	John Stuart Agnew, Marcus Pretzell

<b>0</b>	<b>0</b>

Explicación de los signos utilizados

+ : a favor

- : en contra

0 : abstenciones

## PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EL FONDO

<b>Título</b>	Establecimiento del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y de la Red de Centros Nacionales de Coordinación	
<b>Referencias</b>	COM(2018)0630 – C8-0404/2018 – 2018/0328(COD)	
<b>Fecha de la presentación al PE</b>	12.9.2018	
<b>Comisión competente para el fondo</b> Fecha del anuncio en el Pleno	ITRE 1.10.2018	
<b>Comisiones competentes para emitir opinión</b> Fecha del anuncio en el Pleno	BUDG 1.10.2018	IMCO 1.10.2018
<b>Opinión(es) no emitida(s)</b> Fecha de la decisión	BUDG 9.10.2018	
<b>Ponentes</b> Fecha de designación	Julia Reda 7.11.2018	
<b>Examen en comisión</b>	14.1.2019	
<b>Fecha de aprobación</b>	19.2.2019	
<b>Resultado de la votación final</b>	+	49
	-	2
	0:	6
<b>Miembros presentes en la votación final</b>	Zigmantas Balčytis, Bendt Bendtsen, Xabier Benito Ziluaga, Cristian-Silviu Bușoi, Reinhard Bütikofer, Jerzy Buzek, Angelo Ciocca, Jakop Dalunde, Pilar del Castillo Vera, Christian Ehler, Fredrick Federley, Ashley Fox, Adam Gierek, Theresa Griffin, András Gyürk, Hans-Olaf Henkel, Seán Kelly, Jeppe Kofod, Peter Kouroumbashev, Zdzisław Krasnodębski, Christelle Lechevalier, Janusz Lewandowski, Edouard Martin, Tilly Metz, Angelika Mlinar, Csaba Molnár, Dan Nica, Angelika Niebler, Morten Helveg Petersen, Miroslav Poche, Carolina Punset, Julia Reda, Paul Rübig, Massimiliano Salini, Algirdas Saudargas, Neoklis Sylikiotis, Evžen Tošenovský, Kathleen Van Brempt, Martina Werner, Lieve Wierinck, Hermann Winkler, Anna Záborská, Flavio Zanonato, Carlos Zorrinho	
<b>Suplentes presentes en la votación final</b>	Pilar Ayuso, Michał Boni, Rosa D'Amato, Benedek Jávor, Olle Ludvigsson, Marian-Jean Marinescu, Clare Moody, Markus Pieper, Dominique Riquet, Anneleen Van Bossuyt	
<b>Suplentes (art. 200, apdo. 2) presentes en la votación final</b>	Eleonora Evi, Christelle Lechevalier, Aleksejs Loskutovs, Luigi Morgano	
<b>Fecha de presentación</b>	22.2.2019	

**VOTACIÓN FINAL NOMINAL  
EN LA COMISIÓN COMPETENTE PARA EL FONDO**

<b>49</b>	<b>+</b>
ALDE	Fredrick Federley, Angelika Mlinar, Morten Helveg Petersen, Carolina Punset, Dominique Riquet, Lieve Wierinck
EFDD	Rosa D'Amato, Eleonora Evi
ENF	Christelle Lechevalier
PPE	Pilar Ayuso, Bendt Bendtsen, Michał Boni, Cristian-Silviu Buşoi, Jerzy Buzek, Pilar del Castillo Vera, Christian Ehler, András Gyürk, Seán Kelly, Janusz Lewandowski, Aleksejs Loskutovs, Marian-Jean Marinescu, Angelika Niebler, Markus Pieper, Paul Rübig, Massimiliano Salini, Algirdas Saudargas, Hermann Winkler, Anna Záborská
S&D	Zigmantas Balčytis, Adam Gierek, Theresa Griffin, Jeppe Kofod, Peter Kouroumbashev, Olle Ludvigsson, Edouard Martin, Csaba Molnár, Clare Moody, Luigi Morgano, Dan Nica, Miroslav Poche, Kathleen Van Brempt, Martina Werner, Flavio Zanonato, Carlos Zorrinho
VERTS/ALE	Reinhard Bütikofer, Jakop Dalunde, Benedek Jávor, Tilly Metz, Julia Reda

<b>2</b>	<b>-</b>
GUE/NGL	Xabier Benito Ziluaga, Neoklis Sylikiotis

<b>6</b>	<b>0</b>
ECR	Ashley Fox, Hans-Olaf Henkel, Zdzisław Krasnodębski, Evžen Tošenovský, Anneleen Van Bossuyt
ENF	Angelo Ciocca

Explicación de los signos utilizados

+ : a favor

- : en contra

0 : abstenciones