Consejo de la Unión Europea

Bruselas, 14 de septiembre de 2018
(OR. en)

12104/18

Expediente interinstitucional: 2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	12 de septiembre de 2018
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2018) 630 final
Asunto:	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 *Contribución de la Comisión Europea para la reunión de dirigentes que se celebrará en Salzburgo los días 19 y 20 de septiembre de 2018*

Adjunto se remite a las Delegaciones el documento – COM(2018) 630 final.

Adj.: COM(2018) 630 final

COMISIÓN
EUROPEA

Bruselas, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

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

Contribución de la Comisión Europea para la reunión de dirigentes que se celebrará en Salzburgo los días 19 y 20 de septiembre de 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

A medida que la 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 de la mejora de la capacidad de proteger a la Unión contra las ciberamenazas, ya que tanto la infraestructura civil como las capacidades militares dependen de unos sistemas digitales seguros.

Para hacer frente a los crecientes desafíos, la Unión ha ido incrementando constantemente sus actividades en este ámbito, basándose en la Estrategia de ciberseguridad de 2013[1] y en sus objetivos y principios para fomentar un ecosistema cibernético fiable, seguro y abierto. En 2016, la Unión adoptó sus primeras medidas en el ámbito de la ciberseguridad mediante la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[2] sobre la seguridad de las redes y sistemas de información.

En vista de la rápida evolución del panorama de la ciberseguridad, en septiembre de 2017 la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una Comunicación conjunta[3] titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», con el objetivo de reforzar en mayor medida la resiliencia, la disuasión y la respuesta a los ciberataques. La Comunicación conjunta, basándose también en iniciativas anteriores, describía un conjunto de medidas propuestas que incluían, entre otras, el refuerzo de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), la creación de un marco voluntario de certificación de la ciberseguridad de la UE para mejorar la ciberseguridad de los productos y servicios en el mundo digital, y un plan director para ofrecer una respuesta rápida y coordinada ante los incidentes y crisis de ciberseguridad a gran escala.

En la Comunicación conjunta, se reconocía que también es de interés estratégico para la Unión garantizar que se conservan y desarrollan las capacidades tecnológicas esenciales en materia de ciberseguridad para proteger su mercado único digital y, en particular, para proteger las redes y los sistemas de información fundamentales y prestar servicios clave de ciberseguridad. La Unión debe estar en condiciones de garantizar de forma autónoma la seguridad de sus activos digitales y de competir en el mercado mundial de la ciberseguridad.

En la actualidad, la Unión es un importador neto de productos y soluciones de ciberseguridad y depende en gran medida de proveedores no europeos[4]. El mercado de la ciberseguridad es a nivel mundial un mercado de 600 000 millones EUR que se espera que en los próximos 5 años crezca, de media, aproximadamente un 17 % en términos de ventas, número de empresas

---

1 COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro» [JOIN(2013) 1 final].

2 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).

3 COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO: «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» [JOIN(2017) 450 final].

4 Draft Final Report on the Cybersecurity Market Study [Proyecto de informe final sobre el estudio del mercado de la ciberseguridad], 2018.

y empleo. Sin embargo, entre los veinte países líderes en el ámbito de la ciberseguridad desde el punto de vista del mercado, solo hay seis Estados miembros[5].

Por otra parte, en la Unión hay un buen arsenal de conocimientos especializados y experiencia en materia de ciberseguridad; en efecto, más de 660 organizaciones de toda la Unión Europea (UE) se han inscrito en el reciente inventario de centros especializados en el ámbito de la ciberseguridad llevado a cabo por la Comisión[6]. Estos conocimientos especializados, si se transforman en productos y soluciones comercializables, podrían permitir a la Unión abarcar la totalidad de la cadena de valor de la ciberseguridad. Sin embargo, los esfuerzos de las comunidades investigadora e industrial están fragmentados, no hay armonización ni una misión común, y eso entorpece la competitividad de la UE en este ámbito, así como su capacidad para garantizar la protección de sus activos digitales. En la actualidad, los sectores pertinentes en relación con la ciberseguridad (por ejemplo, la energía, el espacio y el transporte militar), así como sus subsectores, no reciben suficiente apoyo[7]. Las sinergias entre los sectores civil y militar de la ciberseguridad tampoco se explotan plenamente en Europa.

La creación en 2016 de la asociación público-privada («APPc») sobre ciberseguridad en la Unión fue un primer paso firme que reunió a las comunidades investigadora, industrial y del sector público para facilitar la investigación y la innovación en el ámbito de la ciberseguridad y que, dentro de los límites del marco financiero 2014-2020, se espera que dé lugar a resultados positivos y más concretos en materia de investigación e innovación. La APPc hizo posible que los socios industriales manifestaran su compromiso en cuanto al gasto individual en los ámbitos definidos en la agenda estratégica de investigación e innovación de la asociación.

Sin embargo, la Unión puede aspirar a inversiones a una escala mucho mayor y necesita un mecanismo más eficaz que permita crear capacidades duraderas, aunar esfuerzos y competencias, y potenciar el desarrollo de soluciones innovadoras que respondan a los retos industriales relacionados con la ciberseguridad en el campo de las nuevas tecnologías polivalentes (por ejemplo, la inteligencia artificial, la informática cuántica, la cadena de bloques y las identidades digitales seguras), así como en sectores fundamentales (por ejemplo, el transporte, la energía, la salud, el sector financiero, la administración pública, las telecomunicaciones, la industria manufacturera, la defensa o el espacio).

La Comunicación conjunta contemplaba la posibilidad de reforzar la capacidad de ciberseguridad de la Unión a través de una red de centros de competencia en ciberseguridad, con un Centro Europeo de Competencia en Ciberseguridad como eje central. Con ello se pretendía complementar los esfuerzos de creación de capacidades en este ámbito que ya se realizan a nivel nacional y de la Unión. La Comunicación conjunta ponía de manifiesto la intención de la Comisión de iniciar una evaluación de impacto en 2018 para examinar las opciones disponibles con vistas a establecer la estructura. Como primer paso, y para orientar las reflexiones futuras, la Comisión puso en marcha una fase piloto en el marco de Horizonte 2020 con el fin de ayudar a reunir a los centros nacionales en una red y así dar un nuevo impulso en materia de competencia en ciberseguridad y desarrollo tecnológico.

---

5 Draft Final Report on the Cybersecurity Market Study [Proyecto de informe final sobre el estudio del mercado de la ciberseguridad], 2018.

6 Informes técnicos del JRC: European Cybersecurity Centres of Expertise [Centros europeos de conocimientos especializados en ciberseguridad], 2018.

7 Informe técnico del JRC: Outcomes of the Mapping Exercise [Resultados del inventario] (para obtener más detalles, véanse los anexos 4 y 5).

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».

En las Conclusiones del Consejo[8] adoptadas en noviembre de 2017 se pedía a la Comisión que presentara con prontitud una evaluación de impacto sobre las opciones posibles y que propusiera para mediados de 2018 el instrumento jurídico correspondiente para la aplicación de la iniciativa.

El *programa Europa Digital, propuesto por la Comisión en junio de 2018*[9], pretende ampliar y maximizar los beneficios de la transformación digital para los ciudadanos y las empresas europeos en todos los ámbitos políticos pertinentes de la UE, reforzando las políticas y apoyando las ambiciones del mercado único digital. El programa propone un enfoque coherente y global para garantizar el mejor uso posible de las tecnologías avanzadas y la combinación adecuada de capacidad técnica y competencia humana con miras a la transformación digital, no solo en el ámbito de la ciberseguridad, sino también en lo que se refiere a la infraestructura de datos inteligentes, la inteligencia artificial, las capacidades avanzadas y las aplicaciones en la industria y en ámbitos de interés público. Estos elementos son interdependientes, se refuerzan mutuamente y, si se fomentan de manera simultánea, pueden alcanzar la escala necesaria para permitir que prospere una economía de datos[10]. El *programa Horizonte Europa* [11], el próximo Programa Marco de Investigación e Innovación (I+i) de la UE, también sitúa la ciberseguridad entre sus prioridades.

En este contexto, el presente Reglamento propone la creación de un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad junto con una red de Centros Nacionales de Coordinación. Este modelo de cooperación específico debe funcionar como se indica a continuación para estimular el ecosistema europeo tecnológico e industrial en materia de ciberseguridad: el Centro de Competencia facilitará y contribuirá a coordinar el trabajo de la Red y alimentará la Comunidad de Competencias en Ciberseguridad, impulsando el programa tecnológico de ciberseguridad y facilitando el acceso a los conocimientos especializados reunidos de este modo. Para ello, el Centro de Competencia ejecutará, en concreto, las partes pertinentes de los programas Europa Digital y Horizonte Europa, asignando subvenciones y efectuando contrataciones. Habida cuenta de las considerables inversiones en materia de ciberseguridad realizadas en otras partes del mundo y de la necesidad de coordinar y poner en común los recursos necesarios en Europa, se propone que el Centro de Competencia revista la forma de una Asociación Europea[12], de modo que se faciliten las inversiones conjuntas de la Unión, los Estados miembros y la industria. Así pues,

---

8 Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», adoptada por el Consejo de Asuntos Generales el 20 de noviembre de 2017.

9 COM(2018) 434, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027.

10 Véase el documento SWD(2018) 305.

11 COM(2018) 435, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa» y se establecen sus normas de participación y difusión.

12 Tal como se define en el documento COM(2018) 435, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa» y se establecen sus normas de participación y difusión, y se cita en el documento COM(2018) 434, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027.

en la propuesta se pide a los Estados miembros que contribuyan con un importe adecuado a las actuaciones del Centro de Competencia y de la Red. El principal órgano de toma de decisiones es el Consejo de Administración, en el que intervienen todos los Estados miembros, si bien solo tienen derecho a voto los que participan financieramente. El mecanismo de votación utilizado en el Consejo de Administración se rige por un principio de doble mayoría que exige el 75 % de la contribución financiera y el 75 % de los votos. Habida cuenta de su responsabilidad para el presupuesto de la Unión, la Comisión posee el 50 % de los votos. Siempre que resulte apropiado para sus tareas en el Consejo de Administración, la Comisión dispondrá de los conocimientos del Servicio Europeo de Acción Exterior. El Consejo de Administración cuenta con la asistencia de un Consejo Consultivo Industrial y Científico, a fin de garantizar un diálogo sistemático con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes.

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, que trabajaría en estrecha colaboración con la Red de Centros Nacionales de Coordinación y la Comunidad de Competencias en Ciberseguridad (en la que participa un amplio y diverso grupo de agentes implicados en el desarrollo de tecnologías de ciberseguridad, como entidades de investigación, industrias de la oferta, industrias de la demanda y el sector público), creadas por el presente Reglamento, sería el principal organismo de ejecución de los recursos financieros de la UE destinados a la ciberseguridad en el marco del *programa Europa Digital* y del *programa Horizonte Europa* propuestos.

Este enfoque global permitiría apoyar la ciberseguridad en toda la cadena de valor, desde la investigación hasta la implantación y la adopción de tecnologías clave. La participación financiera de los Estados miembros debe ser proporcional a la contribución financiera de la UE a esta iniciativa y constituye un elemento indispensable para su éxito.

Habida cuenta de sus conocimientos especializados y de su amplia y pertinente representación de partes interesadas, conviene invitar a la Organización Europea de Ciberseguridad, que es el homólogo de la Comisión en la asociación público-privada contractual sobre ciberseguridad en el marco de Horizonte 2020, a que contribuya a la labor del Centro y de la Red.

Además, el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad también debe tratar de mejorar las sinergias entre las dimensiones civil y militar de la ciberseguridad. Ha de prestar apoyo a los Estados miembros y a otros agentes oportunos proporcionando asesoramiento, compartiendo conocimientos especializados y facilitando la colaboración en relación con los proyectos y las acciones. Asimismo, a petición de los Estados miembros, podría ejercer de gestor de proyectos, en particular en lo referente al Fondo Europeo de Defensa. La presente iniciativa tiene por objeto contribuir a abordar los siguientes problemas:

- **Insuficiente cooperación entre las industrias de la oferta y la demanda del ámbito de la ciberseguridad.** Las empresas europeas se enfrentan al reto de mantener su seguridad y, al mismo tiempo, ofrecer productos y servicios seguros a sus clientes. Sin embargo, a menudo no son capaces de garantizar adecuadamente la seguridad de los productos, servicios y activos de los que ya disponen o diseñar productos y servicios seguros e innovadores. Los activos clave de ciberseguridad suelen ser demasiado costosos para ser desarrollados e implantados por agentes individuales cuya actividad principal no esté relacionada con la ciberseguridad. Al mismo tiempo, los vínculos entre la oferta y la demanda del mercado de la ciberseguridad no están suficientemente desarrollados, lo que da lugar a una oferta subóptima de productos y soluciones europeos adaptados a las

necesidades de los distintos sectores, así como a un nivel insuficiente de confianza entre los agentes del mercado.

- **Falta de un mecanismo eficiente de cooperación entre los Estados miembros a efectos del desarrollo de capacidades industriales.** Por el momento, tampoco existe un mecanismo eficiente de cooperación para que los Estados miembros colaboren en pos de la creación de las capacidades necesarias para fomentar la innovación en materia de ciberseguridad en los distintos sectores industriales y la implantación de soluciones europeas de ciberseguridad de vanguardia. Los mecanismos de cooperación existentes para los Estados miembros en el ámbito de la ciberseguridad con arreglo a la Directiva (UE) 2016/1148 no prevén este tipo de actividades en su mandato.
- **Cooperación insuficiente en el seno de las comunidades investigadora e industrial y entre ellas.** A pesar de la capacidad teórica de Europa para abarcar la totalidad de la cadena de valor de la ciberseguridad, hay sectores pertinentes en relación con la ciberseguridad (por ejemplo, la energía, el espacio, la defensa o el transporte), así como subsectores, que en la actualidad cuentan con un escaso apoyo de la comunidad investigadora o con el apoyo de un número limitado de centros (por ejemplo, la criptografía cuántica y poscuántica, o la confianza y la ciberseguridad en la inteligencia artificial). Si bien es obvio que existe esta colaboración, por lo general se trata de convenios más bien de asesoramiento y a corto plazo que no permiten emprender planes de investigación a largo plazo para resolver los retos industriales relacionados con la ciberseguridad.
- **Insuficiente cooperación entre las comunidades civil y militar de investigación e innovación en materia de ciberseguridad.** El problema de unos niveles insuficientes de cooperación también afecta a las comunidades civil y militar. Las sinergias existentes no se aprovechan al máximo debido a la falta de mecanismos eficientes que permitan a estas comunidades cooperar con eficiencia y generar confianza, algo que, incluso más que en otros ámbitos, es un requisito previo para el éxito de la cooperación. A ello se añade la limitada capacidad financiera del mercado de la ciberseguridad de la UE, y en particular la falta de fondos para apoyar la innovación.
- **Coherencia con las disposiciones existentes en la misma política sectorial**

La red de competencias en ciberseguridad y el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad servirán de apoyo adicional para las actuales disposiciones políticas del ámbito de la ciberseguridad, así como para sus agentes. El mandato del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad será complementario de los esfuerzos de la ENISA, aunque su enfoque es diferente y requiere un conjunto de capacidades diferente. Mientras que el mandato de la ENISA prevé un papel de asesoramiento sobre investigación e innovación en materia de ciberseguridad en la UE, el mandato propuesto para el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad se centra ante todo en otras funciones cruciales para reforzar la resiliencia en el ámbito de la ciberseguridad en la UE. Además, el mandato de la ENISA no contempla los tipos de actividades, que serían las funciones principales del Centro y de la Red, a saber, estimular el desarrollo y la implantación de la tecnología de ciberseguridad y complementar los esfuerzos de creación de capacidades en este ámbito a escala nacional y de la UE.

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, junto con la red de competencias en ciberseguridad, también trabajará para apoyar la investigación con miras a facilitar y acelerar los procesos de normalización y

certificación, en particular los relacionados con los sistemas de certificación de la ciberseguridad en el sentido del Reglamento de Ciberseguridad propuesto[13][14].

La presente iniciativa supone la ampliación de hecho de la asociación público-privada sobre ciberseguridad (APPc), que fue el primer intento a escala de la UE de reunir a la industria de la ciberseguridad, la parte de la demanda (compradores de productos y soluciones de ciberseguridad, incluidos la administración pública y sectores fundamentales como, por ejemplo, el transporte, la salud, la energía o el sector financiero) y la comunidad investigadora con el objetivo de construir una plataforma de diálogo duradera y crear las condiciones necesarias para la coinversión voluntaria. La APPc se creó en 2016 y generará hasta 1 800 millones EUR de inversión para 2020. Sin embargo, la magnitud de la inversión en curso en otras partes del mundo (por ejemplo, los Estados Unidos invirtieron 19 000 millones USD en ciberseguridad solo en 2017) muestra que la UE debe hacer más para alcanzar una masa crítica de inversión y superar la fragmentación de las capacidades repartidas por toda la UE.

- **Coherencia con otras políticas de la Unión**

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad actuará como organismo único de ejecución de diversos programas de la Unión que apoyan la ciberseguridad (programa Europa Digital y Horizonte Europa) y mejorará la coherencia y las sinergias entre ellos.

Esta iniciativa también permitirá complementar los esfuerzos de los Estados miembros al proporcionar a los responsables de las políticas de educación los recursos adecuados para mejorar las capacidades en materia de ciberseguridad (por ejemplo, mediante el desarrollo de planes de estudios sobre ciberseguridad en los sistemas educativos civil y militar), con el fin de contribuir al desarrollo de una mano de obra cualificada en el ámbito de la ciberseguridad en la UE, lo que constituye un activo fundamental para las empresas de ciberseguridad, así como para otras industrias interesadas en la ciberseguridad. En cuanto educación y formación en ciberdefensa, la presente iniciativa será coherente con el trabajo que está realizando la plataforma sobre educación, formación y ejercicios en ciberdefensa creada al amparo de la Escuela Europea de Seguridad y Defensa.

Esta iniciativa complementará y apoyará los esfuerzos de los centros de innovación digital en el marco del programa Europa Digital. Los centros de innovación digital son organizaciones sin ánimo de lucro que ayudan a las empresas, especialmente las empresas emergentes, las pymes y las empresas de mediana capitalización, a ser más competitivas a través de la mejora de sus actividades empresariales o sus procesos de producción, así como sus productos y servicios, gracias a la innovación inteligente propiciada por la tecnología digital. Los centros de innovación digital proporcionan servicios de innovación orientados a las empresas, tales

---

[13] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad», COM(2017) 477 final/3).

[14] Esto ha de entenderse sin perjuicio de los mecanismos de certificación previstos en el Reglamento general de protección de datos, en los que las autoridades de protección de datos tienen un papel que desempeñar, de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

como información de mercados, asesoramiento financiero, acceso a las instalaciones pertinentes de ensayo y experimentación, formación y desarrollo de capacidades, con el objetivo de ayudar a que los nuevos productos o servicios lleguen con éxito al mercado o introducir mejores procesos de producción. Algunos centros de innovación digital, que disponen de conocimientos especializados en ciberseguridad, podrían participar directamente en la Comunidad de Competencias en Ciberseguridad establecida por la presente iniciativa. Sin embargo, en la mayoría de los casos, los centros de innovación digital, que no tienen un perfil específico de ciberseguridad, facilitarían el acceso de sus miembros a los conocimientos especializados, los conocimientos generales y las capacidades en materia de ciberseguridad disponibles en la Comunidad de Competencias en Ciberseguridad cooperando estrechamente con la Red de Centros Nacionales de Coordinación y el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad. Los centros de innovación digital también apoyarían la implantación de productos y soluciones de ciberseguridad innovadores que respondan a las necesidades de las empresas y otros usuarios finales a los que prestan sus servicios. Por último, los centros de innovación digital específicos de cada sector podrían compartir con la Red y el Centro sus conocimientos acerca de las necesidades reales de los distintos sectores a fin de contribuir a la reflexión sobre una agenda de investigación e innovación que responda a las necesidades industriales.

Se buscarán sinergias con las correspondientes comunidades de conocimiento e innovación del Instituto Europeo de Innovación y Tecnología (EIT), y en particular con el EIT Digital.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

El Centro de Competencia debe establecerse sobre una base jurídica doble debido a su naturaleza y objetivos específicos. El artículo 187 del TFUE, que prevé la creación de las estructuras necesarias para la correcta ejecución de los programas de investigación, desarrollo tecnológico y demostración de la Unión, hace posible que el Centro de Competencia cree sinergias y aúne recursos para invertir en las capacidades necesarias a escala de los Estados miembros y desarrollar activos europeos compartidos (por ejemplo, mediante la adquisición conjunta de la infraestructura necesaria para el ensayo y la experimentación en materia de ciberseguridad). El primer párrafo del artículo 188 prevé la adopción de tales medidas. No obstante, el artículo 188, párrafo primero, como única base jurídica no permitiría que las actividades fueran más allá del ámbito de la investigación y el desarrollo en la medida necesaria para cumplir todos los objetivos del Centro de Competencia que se establecen en el presente Reglamento, de manera que se pueda apoyar la implantación en el mercado de productos y soluciones de ciberseguridad, ayudar a la industria europea de ciberseguridad a ser más competitiva y aumentar su cuota de mercado, y añadir valor a los esfuerzos nacionales dirigidos a solucionar el déficit de capacidades en materia de ciberseguridad. Por lo tanto, para alcanzar estos objetivos, es preciso añadir el artículo 173, apartado 3, como base jurídica que permita a la Unión prever medidas de apoyo a la competitividad del sector.

• Justificación de la propuesta desde el punto de vista de los principios de subsidiariedad y proporcionalidad

La ciberseguridad es una cuestión de interés común para la Unión, tal y como lo confirman las Conclusiones del Consejo mencionadas anteriormente. Por otra parte, se han de tener en cuenta la magnitud y el carácter transfronterizo de incidentes como los de WannaCry o NonPetya. La naturaleza y la magnitud de los retos tecnológicos en materia de ciberseguridad, así como la insuficiente coordinación de los esfuerzos tanto dentro de la industria, el sector

público y la comunidad investigadora como entre estas partes, exigen que la UE apoye en mayor medida los esfuerzos de coordinación a fin de poner en común una masa crítica de recursos y garantizar una mejor gestión de los conocimientos y los activos. Esto es necesario en vista de las exigencias de recursos en relación con determinadas capacidades para la investigación, el desarrollo y la implantación de la ciberseguridad; la necesidad de proporcionar acceso a conocimientos prácticos e interdisciplinares sobre ciberseguridad en diferentes disciplinas (a menudo solo parcialmente disponibles a nivel nacional); la naturaleza mundial de las cadenas de valor industriales, y la actividad de los competidores mundiales que están presentes en todos los mercados.

Para ello se requieren recursos y conocimientos especializados a una escala que difícilmente puede ser igualada por la acción individual de ningún Estado miembro. Por ejemplo, una red paneuropea de comunicación cuántica podría requerir una inversión de la UE de aproximadamente 900 millones EUR, en función de las inversiones de los Estados miembros (que habrá que interconectar/complementar) y de la medida en que la tecnología permita la reutilización de las infraestructuras existentes. La iniciativa será decisiva para poner en común la financiación y permitir que este tipo de inversión se realice en la Unión.

Los objetivos de la presente iniciativa no pueden ser alcanzados plenamente por los Estados miembros por sí solos. Como se ha indicado anteriormente, pueden lograrse mejor a nivel de la Unión, aunando esfuerzos y evitando su duplicación innecesaria, contribuyendo a alcanzar una masa crítica de inversión y garantizando una utilización óptima de la financiación pública. Al mismo tiempo, de conformidad con el principio de proporcionalidad, el presente Reglamento no excede de lo necesario para alcanzar ese objetivo. Por lo tanto, la acción de la UE está justificada en cuanto a la subsidiariedad y la proporcionalidad.

El presente instrumento no prevé nuevas obligaciones normativas para las empresas. Por otra parte, es probable que las empresas, y especialmente las pymes, reduzcan los costes relacionados con sus esfuerzos para el diseño de productos seguros desde el punto de vista cibernético e innovadores, ya que la iniciativa permite poner en común recursos para invertir en las capacidades necesarias a nivel de los Estados miembros o desarrollar activos europeos compartidos (por ejemplo, adquiriendo conjuntamente la infraestructura necesaria para el ensayo y la experimentación en relación con la ciberseguridad). Estos activos podrían ser utilizados por las industrias y las pymes de diferentes sectores a fin de garantizar que sus productos son seguros desde el punto de vista cibernético y convertir la ciberseguridad en su ventaja competitiva.

- **Elección del instrumento**

El instrumento propuesto establece un organismo dedicado a la ejecución de acciones en materia de ciberseguridad en el marco del programa Europa Digital y el programa Horizonte Europa. Describe su mandato, sus funciones y su estructura de gobernanza. La creación de tal organismo de la Unión requiere la adopción de un Reglamento.

3. CONSULTAS CON LAS PARTES INTERESADAS Y EVALUACIONES DE IMPACTO

La propuesta de crear una red de competencias en ciberseguridad junto con un Centro Europeo de Investigación y Competencia en Ciberseguridad es una iniciativa nueva. Supone la continuación y ampliación de la asociación público-privada contractual sobre ciberseguridad creada en 2016.

- **Consultas con las partes interesadas**

La ciberseguridad es un tema amplio e intersectorial. La Comisión ha utilizado diferentes métodos de consulta para asegurarse de que el interés público general de la Unión, en contraposición a los intereses especiales de un abanico reducido de grupos de partes interesadas, queda debidamente reflejado en la presente iniciativa. Este método garantiza la transparencia y la rendición de cuentas en la labor de la Comisión. Aunque no se ha llevado a cabo ninguna consulta pública abierta específicamente para la presente iniciativa dado su público destinatario (la comunidad industrial e investigadora y los Estados miembros), el tema ya ha sido objeto de varias consultas públicas abiertas:

- Una consulta pública abierta general realizada en 2018 sobre el ámbito de la inversión, la investigación y la innovación, las pymes y el mercado único.
- En 2017 se puso en marcha una consulta pública en línea de doce semanas de duración para recabar las opiniones del público en general (aproximadamente noventa encuestados) sobre la evaluación y revisión de la ENISA.
- En 2016 se realizó una consulta pública en línea de doce semanas de duración con motivo del lanzamiento de la asociación público-privada contractual sobre ciberseguridad (aproximadamente doscientos cuarenta encuestados).

Por otra parte, la Comisión ha organizado consultas específicas sobre la iniciativa, incluidos talleres, reuniones y solicitudes específicas de información (de parte de la ENISA y de la Agencia Europea de Defensa). El período de consulta se extendió a lo largo de seis meses, desde noviembre de 2017 hasta marzo de 2018. Asimismo, la Comisión ha efectuado un inventario de los centros de conocimientos especializados que ha permitido recabar información de 665 centros de conocimientos especializados en ciberseguridad acerca de sus conocimientos prácticos, su actividad, sus ámbitos de trabajo y su cooperación internacional. La encuesta comenzó en enero, y se han tenido en cuenta las respuestas presentadas hasta el 8 de marzo de 2018 para el análisis.

Las partes interesadas de los sectores industrial e investigador consideran que el Centro de Competencia y la Red podrían añadir valor a los esfuerzos actuales a nivel nacional al ayudar a crear un ecosistema de ciberseguridad a escala europea que haga posible una mejor cooperación entre las comunidades investigadora e industrial. También consideran necesario que la UE y los Estados miembros adopten una perspectiva proactiva, a más largo plazo y estratégica respecto de la política industrial en materia de ciberseguridad que vaya más allá de la investigación y la innovación. Las partes interesadas han puesto de manifiesto la necesidad de acceder a capacidades clave, como instalaciones de ensayo y experimentación, así como la necesidad de ser más ambiciosos a la hora de colmar el déficit de capacidades en materia de ciberseguridad, por ejemplo, mediante proyectos europeos a gran escala que atraigan a los mejores talentos. Todo lo anterior también se considera necesario para que la Unión sea reconocida mundialmente como un líder en ciberseguridad.

Los Estados miembros, en el marco de las actividades de consulta emprendidas desde el pasado mes de septiembre[15], así como en las Conclusiones específicas del Consejo[16], han acogido con satisfacción la intención de crear una red de competencias en ciberseguridad para

[15] Por ejemplo, la Mesa Redonda de Alto Nivel con los Estados miembros, el vicepresidente Ansip y la comisaria Gabriel, el 5 de diciembre de 2017.

[16] Consejo de Asuntos Generales: Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» (20 de noviembre de 2017).

estimular el desarrollo y la implantación de las tecnologías de ciberseguridad, pero han subrayado la necesidad de incluir a todos los Estados miembros y sus centros de excelencia y competencia existentes, así como de prestar especial atención a la complementariedad. En lo que se refiere específicamente al futuro Centro de Competencia, los Estados miembros han recalcado la importancia de su función de coordinación en apoyo a la red. En particular, respecto a las actividades y necesidades nacionales de ciberdefensa, el inventario sobre las necesidades en ciberdefensa de los Estados miembros realizado por el Servicio Europeo de Acción Exterior en marzo de 2018 demostró que la mayoría de los Estados miembros perciben el valor añadido de la ayuda de la UE para ciberformación y cibereducación, así como del apoyo a la industria a través de la investigación y el desarrollo[17]. En efecto, la iniciativa se llevaría a cabo en colaboración con los Estados miembros o las entidades apoyadas por ellos. La colaboración entre la industria, la comunidad investigadora y la comunidad del sector público haría posible reforzar y agrupar a las entidades existentes e intensificar y aunar los esfuerzos actuales con el fin de evitar duplicaciones. Los Estados miembros también participarían en la definición de acciones específicas dirigidas al sector público como usuario directo de la tecnología y los conocimientos prácticos en materia de ciberseguridad.

- **Evaluación de impacto**

El 11 de abril de 2017 se presentó al Comité de Control Reglamentario una evaluación de impacto en apoyo de la presente iniciativa, que recibió un dictamen positivo con reservas. La evaluación de impacto se revisó posteriormente a la luz de las observaciones del Comité. El dictamen del Comité y el anexo en el que se explica de qué modo se tuvieron en cuenta sus observaciones se publican conjuntamente con la presente propuesta.

En la evaluación de impacto se consideraron varias opciones políticas, tanto legislativas como no legislativas. Se escogieron las siguientes opciones para una evaluación a fondo:

- La hipótesis de referencia (opción de colaboración) supone la continuación del enfoque actual de creación de capacidades industriales y tecnológicas de ciberseguridad en la UE mediante el apoyo a la investigación y la innovación y los mecanismos de colaboración conexos en el marco del 9PM.
- Opción 1: Red de competencias en ciberseguridad, junto con un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad con el doble mandato de aplicar medidas de apoyo a las tecnologías industriales y en el ámbito de la investigación y la innovación.
- Opción 2: Red de competencias en ciberseguridad, junto con un Centro Europeo de Investigación y Competencia en Ciberseguridad centrado en actividades de investigación e innovación.

Entre las opciones descartadas en una fase inicial figuraban: 1) la opción de no adoptar ninguna medida, 2) la opción de crear únicamente la red de competencias en ciberseguridad, 3) la opción de crear únicamente una estructura centralizada, y 4) la opción de recurrir a una agencia existente (Agencia Europea de Seguridad de las Redes y de la Información de la UE, ENISA; Agencia Ejecutiva de Investigación, REA, o Agencia Ejecutiva de Innovación y Redes, INEA).

[17] SEAE, marzo de 2018.

El análisis llegó a la conclusión de que la opción 1 es la más adecuada para alcanzar los objetivos de la iniciativa, al tiempo que ofrece la mayor repercusión económica, social y medioambiental y salvaguarda los intereses de la Unión. Los principales argumentos a favor de esta opción son la capacidad para crear una auténtica política industrial de ciberseguridad apoyando actividades relacionadas no solo con la investigación y el desarrollo, sino también con la implantación en el mercado; la flexibilidad para permitir diferentes modelos de cooperación con la red de centros de competencia y de ese modo optimizar el uso de los conocimientos y recursos existentes; y la capacidad para estructurar la cooperación y los compromisos conjuntos de las partes interesadas, públicas y privadas, de todos los sectores oportunos, incluido el de la defensa. Por último, la opción 1 también permite aumentar las sinergias y puede servir de mecanismo de aplicación para dos fuentes diferentes de financiación de la UE en materia de ciberseguridad en el próximo marco financiero plurianual (el programa Europa Digital y Horizonte Europa).

- **Derechos fundamentales**

La presente iniciativa permitirá a las autoridades públicas y las industrias de todos los Estados miembros prevenir y actuar ante las ciberamenazas de manera más eficaz ofreciendo y equipándose con productos y soluciones más seguros. Esto es especialmente importante de cara a la protección del acceso a los servicios esenciales (por ejemplo, el transporte, la salud, la banca y los servicios financieros).

El incremento de la capacidad de la Unión Europea para garantizar de forma autónoma la seguridad de sus productos y servicios también puede ayudar a los ciudadanos a disfrutar de sus derechos y valores democráticos (por ejemplo, mediante una mejor protección de sus derechos relacionados con la información y consagrados en la Carta de los Derechos Fundamentales, en particular el derecho a la protección de los datos personales y la privacidad) y, en consecuencia, aumentar su confianza en la sociedad y la economía digitales.

4. REPERCUSIONES PRESUPUESTARIAS

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, en cooperación con la red de competencias en ciberseguridad, será el principal organismo de ejecución de los recursos financieros de la UE destinados a la ciberseguridad en el marco de Europa Digital y Horizonte Europa.

Las implicaciones presupuestarias relacionadas con la ejecución de Europa Digital se recogen detalladamente en la ficha financiera legislativa aneja a la presente propuesta. La contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), será propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político. La propuesta se basará en los resultados del proceso de planificación estratégica definido en el artículo 6, apartado 6, del Reglamento XXX [programa marco Horizonte Europa].

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

En la presente propuesta se prevé una cláusula explícita de evaluación, en virtud de la que la Comisión llevará a cabo una evaluación independiente (artículo 38). Posteriormente, la Comisión informará al Parlamento Europeo y al Consejo de su evaluación, adjuntando,

cuando proceda, una propuesta de revisión, a fin de medir la repercusión del instrumento y su valor añadido. Se aplicará la metodología de evaluación contenida en el Reglamento sobre la mejora de la legislación de la Comisión.

El director ejecutivo debe presentar cada dos años al Consejo de Administración una evaluación *ex post* de las actividades del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y de la Red, tal como se establece en el artículo 17 de la presente propuesta. El director ejecutivo debe, asimismo, elaborar un plan de actuación para dar seguimiento a las conclusiones de las evaluaciones retrospectivas e informar dos veces al año a la Comisión sobre los progresos realizados. El Consejo de Administración ha de ser responsable de supervisar que se da el seguimiento adecuado a dichas conclusiones, como se dispone en el artículo 16 de la presente propuesta.

Los supuestos casos de mala administración en las actividades de la entidad jurídica podrán estar sujetos a investigaciones del Defensor del Pueblo Europeo de conformidad con lo dispuesto en el artículo 228 del Tratado.

2018/0328 (COD)

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

Contribución de la Comisión Europea para la reunión de dirigentes que se celebrará en Salzburgo los días 19 y 20 de septiembre de 2018

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 173, apartado 3, y su artículo 188, párrafo primero,

Vista la propuesta de la Comisión Europea,

Visto el dictamen del Comité Económico y Social Europeo[18],

Visto el dictamen del Comité de las Regiones[19],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(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.

(2) La Unión ha ido incrementando de forma constante sus actividades dirigidas a hacer frente a los crecientes desafíos en materia de ciberseguridad, de conformidad con la Estrategia de Ciberseguridad de 2013[20], cuyo objetivo es fomentar un ecosistema cibernético fiable, seguro y abierto. En 2016, la Unión adoptó las primeras medidas en el ámbito de la ciberseguridad mediante la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[21] sobre la seguridad de las redes y sistemas de información.

---

18 DO C […] de […], p. […].

19 DO C […] de […], p. […].

20 Comunicación conjunta al Parlamento Europeo y al Consejo: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro» [JOIN(2013) 1 final].

21 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).

(3) En septiembre de 2017, la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una Comunicación conjunta[22] titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», con el objetivo de reforzar en mayor medida la resiliencia, la disuasión y la respuesta a los ciberataques.

(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».

(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 prestar servicios clave de ciberseguridad.

(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.

(7) En las Conclusiones del Consejo adoptadas en noviembre de 2017 se pedía a la Comisión que presentara con prontitud una evaluación de impacto sobre las opciones posibles para crear una red de centros de competencia en ciberseguridad junto con un Centro Europeo de Competencia e Investigación, y que propusiera para mediados de 2018 el instrumento jurídico correspondiente.

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

(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

[22] Comunicación conjunta al Parlamento Europeo y al Consejo: «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» [JOIN(2017) 450 final].

financieramente a los costes administrativos y de funcionamiento del Centro de Competencia deben tener derecho de voto.

(10) La contribución financiera de los Estados miembros participantes ha de ser proporcional a la contribución financiera de la Unión a la presente iniciativa.

(11) El Centro de Competencia debe facilitar y ayudar a coordinar la labor de la red de competencias en ciberseguridad (en lo sucesivo, la «Red»), compuesta por los centros nacionales de coordinación de los distintos Estados miembros. Es preciso que los centros nacionales de coordinación reciban apoyo financiero directo de la Unión, incluida la concesión de subvenciones sin convocatoria de propuestas, para llevar a cabo actividades relacionadas con el presente Reglamento.

(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[23], y la comunidad investigadora.

(13) Cuando se proporcione ayuda financiera a los centros nacionales de coordinación para apoyar a terceros en el ámbito nacional, esta ayuda se transmitirá a las partes interesadas correspondientes mediante acuerdos de subvención en cascada.

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

(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

[23] 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).

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.

(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.

(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.

(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.

(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.

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

(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.

(22) Cuando reciban una contribución financiera con cargo al presupuesto general de la Unión, los centros nacionales de coordinación y las entidades que formen parte de la Comunidad de Competencias en Ciberseguridad han de dar a conocer el hecho de que las respectivas actividades se llevan a cabo en el marco de la presente iniciativa.

(23) La contribución de la Unión al Centro de Competencia debe financiar la mitad de los costes derivados de las actividades de creación, administración y coordinación de este centro. Por otra parte, con miras a evitar la doble financiación, estas actividades no han de recibir simultáneamente ninguna contribución de otros programas de la Unión.

(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.

(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.

(26) En aras del buen funcionamiento del Centro de Competencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión, debidamente acreditada, así como a su competencia y experiencia en relación con la ciberseguridad. También es necesario que desempeñe sus funciones con completa independencia.

(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.

(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.

(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 acceso del público a los documentos, según se establece en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo[24]. 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.

(30) Es necesario proteger los intereses financieros de la Unión y de los Estados miembros con medidas proporcionadas a lo largo de todo el ciclo de gasto, lo que incluye la

[24] 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).

prevención, la detección y la investigación de irregularidades, la recuperación de los fondos perdidos, pagados por error o utilizados de forma incorrecta, y, en su caso, la aplicación de sanciones administrativas y financieras de conformidad con el Reglamento XXX (UE, Euratom) del Parlamento Europeo y del Consejo[25] (el Reglamento Financiero).

(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.

(32) El auditor interno de la Comisión ha de desempeñar respecto al Centro de Competencia las mismas funciones que respecto a la Comisión.

(33) La Comisión, el Centro de Competencia, el Tribunal de Cuentas y la Oficina Europea de Lucha contra el Fraude deben tener acceso a toda la información necesaria y a los locales para llevar a cabo auditorías e investigaciones sobre las subvenciones, los contratos y los acuerdos firmados por el Centro de Competencia.

(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 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.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES Y PRINCIPIOS GENERALES DEL CENTRO DE COMPETENCIA Y LA RED

Artículo 1

Objeto

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.

[25] [añadir título y referencia del DO]

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 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].

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

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.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

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

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;

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;

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

Artículo 3

Misión del Centro y de la Red

1. El Centro de Competencia y la Red ayudarán a la Unión a lo siguiente:

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

   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.

2. El Centro de Competencia desempeñará sus funciones, cuando proceda, en colaboración con la Red de Centros Nacionales de Coordinación y una Comunidad de Competencias en Ciberseguridad.

Artículo 4

Objetivos y funciones del Centro

El Centro de Competencia tendrá los objetivos y las funciones conexas siguientes:

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;

2. contribuir a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX[26], 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[27], 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];

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:

    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;

    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;

    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;

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:

    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;

    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;

---

26 [añadir título completo y referencia del DO]

27 [añadir título completo y referencia del DO]

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;

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;

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:

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;

6. contribuir a reforzar la investigación y el desarrollo en materia de ciberseguridad en la Unión a través de lo siguiente:

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;

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;

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

7. reforzar la cooperación entre las esferas civil y militar en lo que se refiere a las tecnologías y aplicaciones de doble uso en ciberseguridad a través de lo siguiente:

a) apoyar a los Estados miembros y a las partes interesadas de la industria y del ámbito investigador en lo referente a la investigación, el desarrollo y la implantación;

b) contribuir a la cooperación entre los Estados miembros mediante el apoyo a la educación, la formación y los ejercicios;

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

8. reforzar las sinergias entre las dimensiones civil y militar de la ciberseguridad en relación con el Fondo Europeo de Defensa a través de lo siguiente:

a) proporcionar asesoramiento, compartir conocimientos especializados y facilitar la colaboración entre las partes interesadas pertinentes;

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].

Artículo 5

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

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:

   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 el Centro de Competencia defina;

   b) las normas por las que se regirán el acceso a una infraestructura o capacidad y su uso.

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.

Artículo 6

Designación de los centros nacionales de coordinación

1. A más tardar el [fecha], cada Estado miembro designará a la entidad que ejercerá las funciones de centro nacional de coordinación a efectos del presente Reglamento y lo notificará a la Comisión.

2. Sobre la base de una evaluación de la conformidad de dicha entidad con los criterios establecidos en el apartado 4, la Comisión emitirá una decisión en el plazo de seis meses a partir de la propuesta transmitida por el Estado miembro en la que se dispondrá la acreditación de la entidad como centro nacional de coordinación o se rechazará la designación. La Comisión publicará la lista de centros nacionales de coordinación.

3. Los Estados miembros podrán designar en cualquier momento una nueva entidad como centro nacional de coordinación a efectos del presente Reglamento. Los apartados 1 y 2 se aplicarán a la designación de toda nueva entidad.

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.

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.

6. La Red de Centros Nacionales de Coordinación estará compuesta por todos los centros nacionales de coordinación designados por los Estados miembros.

Artículo 7

Funciones de los centros nacionales de coordinación

1. Los centros nacionales de coordinación tendrán las siguientes funciones:

   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;

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

   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;

   d) ejercer de punto de contacto a escala nacional para la Comunidad de Competencias en Ciberseguridad y el Centro de Competencia;

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

   f) ejecutar acciones específicas subvencionadas por el Centro de Competencia, incluido mediante la concesión de ayuda financiera a terceros, de conformidad con el artículo 204 del Reglamento XXX (nuevo Reglamento Financiero), en las condiciones especificadas en el acuerdo de subvención correspondiente;

   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;

   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.

2. A efectos de la letra f), la ayuda financiera a terceros podrá prestarse en cualquiera de las formas especificadas en el artículo 125 del Reglamento XXX [nuevo Reglamento Financiero], incluido en forma de cantidades fijas únicas.

3. Los centros nacionales de coordinación podrán recibir una subvención de la Unión, de conformidad con el artículo 195, letra d), del Reglamento XXX [nuevo Reglamento Financiero], para la realización de las funciones establecidas en el presente artículo.

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).

Artículo 8

Comunidad de Competencias en Ciberseguridad

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.

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.

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:

   a) investigación;

   b) desarrollo industrial;

   c) formación y educación.

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].

5. El Centro de Competencia acreditará a los órganos y organismos oportunos de la Unión como miembros de la Comunidad de Competencias en Ciberseguridad tras evaluar si la entidad en cuestión cumple los criterios establecidos en el apartado 3. La acreditación no tendrá una duración limitada, pero podrá ser revocada por el Centro de Competencia en cualquier momento si 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].

6. Los representantes de la Comisión podrán participar en la labor de la Comunidad.

Artículo 9

Funciones de los miembros de la Comunidad de Competencias en Ciberseguridad

Los miembros de la Comunidad de Competencias en Ciberseguridad:

1) apoyarán al Centro de Competencia en pos del cumplimiento de la misión y los objetivos establecidos en los artículos 3 y 4, y, a tal fin, trabajarán en estrecha colaboración con el Centro de Competencia y los centros nacionales de coordinación de que se trate;

2) participarán en las actividades promovidas por el Centro de Competencia y los centros nacionales de coordinación;

3) cuando proceda, participarán en los grupos de trabajo establecidos por el Consejo de Administración del Centro de Competencia para llevar a cabo actividades específicas con arreglo al plan de trabajo del Centro de Competencia;

4) cuando proceda, apoyarán al Centro de Competencia y a los centros nacionales de coordinación en la promoción de proyectos específicos;

5) promoverán y difundirán los resultados pertinentes de las actividades y proyectos llevados a cabo en la Comunidad.

Artículo 10

Cooperación del Centro de Competencia con las instituciones, los órganos y los organismos de la Unión

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.

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.

CAPÍTULO II

ORGANIZACIÓN DEL CENTRO DE COMPETENCIA

Artículo 11

Miembros y estructura

1. Los miembros del Centro de Competencia serán la Unión, representada por la Comisión, y los Estados miembros.

2. La estructura del Centro de Competencia comprenderá lo siguiente:

a) un Consejo de Administración, que ejercerá las funciones establecidas en el artículo 13;

b) un director ejecutivo, que ejercerá las funciones establecidas en el artículo 16;

c) un Consejo Consultivo Industrial y Científico, que ejercerá las funciones definidas en el artículo 20.

SECCIÓN I

CONSEJO DE ADMINISTRACIÓN

Artículo 12

Composición del Consejo de Administración

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.

2. Cada miembro del Consejo de Administración tendrá un suplente que le representará en su ausencia.

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.

4. El mandato de los miembros del Consejo de Administración y sus suplentes será de cuatro años. Este mandato será renovable.

5. Los miembros del Consejo de Administración actuarán con independencia y transparencia, en interés del Centro de Competencia, salvaguardando sus objetivos, así como su misión, identidad, autonomía y coherencia.

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.

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.

Artículo 13

Funciones del Consejo de Administración

1. El Consejo de Administración asumirá la responsabilidad general respecto de la orientación estratégica y las operaciones del Centro de Competencia y supervisará la ejecución de sus actividades.

2. El Consejo de Administración adoptará su reglamento interno. En estas normas se incluirán procedimientos específicos para identificar y evitar los conflictos de intereses y garantizar la confidencialidad de la información delicada.

3. El Consejo de Administración adoptará las decisiones estratégicas necesarias, y en particular:

   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;

   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;

   c) adoptará las normas financieras específicas del Centro de Competencia de conformidad con el [artículo 70 del Reglamento Financiero];

   d) adoptará un procedimiento para el nombramiento del director ejecutivo;

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

   f) nombrará al director ejecutivo, lo destituirá, ampliará su mandato, le asesorará y supervisará su rendimiento, y nombrará al contable;

   g) aprobará el presupuesto anual del Centro de Competencia, incluida la plantilla de personal correspondiente, donde se indicará el número de puestos

temporales por grupo de funciones y por grado, así como el número de personas contratadas y de expertos nacionales en comisión de servicios, expresado en equivalentes a jornada completa;

h) adoptará las normas relativas a los conflictos de intereses;

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

j) nombrará a los miembros del Consejo Consultivo Industrial y Científico;

k) establecerá una función de auditoría interna de conformidad con el Reglamento Delegado (UE) n.º 1271/2013 de la Comisión[28];

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;

m) establecerá la política de comunicación del Centro de Competencia a recomendación del director ejecutivo;

n) será responsable de supervisar que se da el seguimiento adecuado a las conclusiones de las evaluaciones retrospectivas;

o) cuando proceda, adoptará normas de desarrollo del Estatuto de los funcionarios y el régimen aplicable a los otros agentes, de conformidad con lo dispuesto en el artículo 31, apartado 3;

p) cuando proceda, establecerá normas sobre la designación de expertos nacionales en comisión de servicios en el Centro de Competencia y sobre el recurso a personal en prácticas, de conformidad con lo dispuesto en el artículo 32, apartado 2;

q) adoptará normas de seguridad para el Centro de Competencia;

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 vayan a aplicarse;

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

t) será responsable de cualquier función no encomendada específicamente a un órgano concreto del Centro de Competencia; podrá asignar estas funciones a cualquier persona del Centro de Competencia.

Artículo 14

Presidente y reuniones del Consejo de Administración

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

[28] Reglamento Delegado (UE) n.º 1271/2013 de la Comisión, de 30 de septiembre de 2013, relativo al Reglamento Financiero marco de los organismos a que se refiere el artículo 208 del Reglamento (UE, Euratom) n.º 966/2012 del Parlamento Europeo y del Consejo (DO L 328 de 7.12.2013, p. 42).

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.

2. El Consejo de Administración celebrará reuniones ordinarias al menos tres veces al año. Podrá celebrar reuniones extraordinarias a petición de la Comisión, a petición de un tercio de sus miembros, a petición del presidente o a petición del director ejecutivo en el ejercicio de sus funciones.

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.

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.

5. Los miembros del Consejo de Administración y sus suplentes podrán, a reserva de su reglamento interno, estar asistidos en las reuniones por asesores o expertos.

6. El Centro de Competencia se encargará de la secretaría del Consejo de Administración.

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.

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.

SECCIÓN II

DIRECTOR EJECUTIVO

Artículo 16

Nombramiento, destitución o ampliación del mandato del director ejecutivo

1. El director ejecutivo será una persona con conocimientos especializados y una gran reputación en los ámbitos en los que actúe el Centro de Competencia.

2. El director ejecutivo será contratado como agente temporal del Centro de Competencia según lo dispuesto en el artículo 2, letra a), del régimen aplicable a los otros agentes.

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.

4. A efectos de la celebración del contrato del director ejecutivo, el Centro de Competencia estará representado por el presidente del Consejo de Administración.

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.

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.

7. El director ejecutivo cuyo mandato haya sido ampliado no podrá participar en otro procedimiento de selección para el mismo puesto.

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

Artículo 17

Funciones del director ejecutivo

1. El director ejecutivo será responsable de las operaciones y la gestión cotidiana del Centro de Competencia, y será su representante legal. La persona que desempeñe este cargo responderá ante el Consejo de Administración y llevará a cabo sus funciones con total independencia dentro de las competencias que le hayan sido asignadas.

2. En particular, el director ejecutivo realizará las siguientes tareas de forma independiente:

   a) ejecutar las decisiones adoptadas por el Consejo de Administración;

   b) apoyar la labor del Consejo de Administración, hacerse cargo de la secretaría de sus reuniones y proporcionar toda la información necesaria para el desempeño de sus funciones;

   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;

   d) elaborar y presentar al Consejo de Administración, para su adopción, el proyecto de presupuesto anual, incluida la plantilla de personal correspondiente, en la que se indicará el número de puestos temporales por grupo de función y grado, así como el número de personas contratadas y de expertos nacionales en comisión de servicios, expresado en equivalentes a jornada completa;

e) ejecutar el plan de trabajo e informar al Consejo de Administración al respecto;

f) elaborar el proyecto de informe anual de actividades relativo al Centro de Competencia, incluida la información sobre los gastos correspondientes;

g) garantizar la aplicación de procedimientos eficaces de seguimiento y evaluación de los resultados del Centro de Competencia;

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;

i) elaborar, negociar y celebrar los acuerdos con los centros nacionales de coordinación;

j) responsabilizarse de las cuestiones administrativas, financieras y de personal, incluida la ejecución del presupuesto del Centro de Competencia, teniendo debidamente en cuenta el asesoramiento recibido de parte de la función de auditoría interna, dentro de los límites de la delegación del Consejo de Administración;

k) aprobar y gestionar la publicación de las convocatorias de propuestas, de conformidad con el plan de trabajo, y administrar los acuerdos y decisiones de subvención;

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

m) aprobar y gestionar la publicación de las convocatorias de licitación, de conformidad con el plan de trabajo, y administrar los contratos;

n) aprobar las ofertas seleccionadas para su financiación;

o) presentar el proyecto de cuentas y balance anuales a la función de auditoría interna y, posteriormente, al Consejo de Administración;

p) velar por que se lleven a cabo la evaluación y gestión de riesgos;

q) firmar los acuerdos, decisiones y contratos de subvención específicos;

r) firmar contratos públicos;

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;

t) elaborar el proyecto de normas financieras aplicables al Centro de Competencia;

u) crear un sistema de control interno eficaz y eficiente, y garantizar su funcionamiento, así como informar al Consejo de Administración de cualquier cambio significativo que se produzca en él;

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

w) adoptar cualquier otra medida necesaria para evaluar los avances del Centro de Competencia en pos de la consecución de su misión y objetivos, tal como se establece en los artículos 3 y 4 del presente Reglamento;

x) llevar a cabo las demás funciones que le sean encomendadas o delegadas por el Consejo de Administración.

SECCIÓN III

CONSEJO CONSULTIVO INDUSTRIAL Y CIENTÍFICO

Artículo 18

Composición del Consejo Consultivo Industrial y Científico

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 Ciberseguridad.
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.
3. Los procedimientos relativos al nombramiento de sus miembros por el Consejo de Administración y al funcionamiento del Consejo Consultivo se especificarán en el reglamento interno del Centro de Competencia y se harán públicos.
4. El mandato de los miembros del Consejo Consultivo Industrial y Científico tendrá una duración de tres años. Este mandato será renovable.
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.

Artículo 19

Funcionamiento del Consejo Consultivo Industrial y Científico

1. El Consejo Consultivo Industrial y Científico se reunirá como mínimo dos veces al año.
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.
3. El Consejo Consultivo Industrial y Científico elegirá a su presidente.
4. El Consejo Consultivo Industrial y Científico adoptará su reglamento interno, incluido el nombramiento de quienes, cuando proceda, lo representarán, así como la duración de tal nombramiento.

Artículo 20

Funciones del Consejo Consultivo Industrial y Científico

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

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;

2) organizar consultas públicas abiertas a todas las partes interesadas de los sectores público y privado relacionadas con el ámbito de la ciberseguridad, a fin de recabar información para el asesoramiento estratégico a que se refiere el punto 1;

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

CAPÍTULO III
DISPOSICIONES FINANCIERAS

Artículo 21

Contribución financiera de la Unión

1. La contribución de la Unión al Centro de Competencia para cubrir los gastos administrativos y los gastos de funcionamiento comprenderá lo siguiente:

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

   b) un importe del programa Horizonte Europa, incluido para gastos administrativos, que se determinará teniendo en cuenta el proceso de planificación estratégica que debe llevarse a cabo de conformidad con el artículo 6, apartado 6, del Reglamento XXX [Reglamento relativo a Horizonte Europa].

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

3. El Centro de Competencia ejecutará las acciones de ciberseguridad del [programa Europa Digital] y el [programa Horizonte Europa], de conformidad con el artículo 62, letra c), inciso iv), del Reglamento (UE, Euratom) XXX[29] [Reglamento Financiero].

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

Artículo 22

Contribuciones de los Estados miembros participantes

1. Los Estados miembros participantes aportarán una contribución total a los gastos de funcionamiento y administrativos del Centro de Competencia que será como mínimo igual a los importes que se indican en el artículo 21, apartado 1, del presente Reglamento.

[29] [añadir título completo y referencia del DO]

2. A efectos de establecer las contribuciones contempladas en el apartado 1 y en el artículo 23, apartado 3, letra b), inciso ii), los gastos se determinarán de conformidad con las prácticas contables habituales en materia de gastos de los Estados miembros de que se trate, las normas de contabilidad aplicables del Estado miembro y las Normas Internacionales de Contabilidad y las Normas Internacionales de Información Financiera aplicables. Un auditor externo independiente nombrado por el Estado miembro de que se trate certificará los gastos. El Centro de Competencia podrá verificar el método de valoración en caso de surgir dudas en relación con la certificación.

3. Si algún Estado miembro participante incumple sus compromisos en lo que se refiere a las contribuciones financieras, el director ejecutivo lo notificará por escrito y fijará un plazo razonable para que se subsane dicho incumplimiento. Si el incumplimiento no se subsana en el plazo fijado, el director ejecutivo convocará una reunión del Consejo de Administración para decidir si debe revocarse el derecho de voto del Estado miembro participante en cuestión o si deben adoptarse otras medidas hasta que dicho Estado miembro haya cumplido con sus obligaciones. Asimismo, los derechos de voto de este Estado miembro quedarán suspendidos hasta que no subsane el incumplimiento.

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.

5. Los Estados miembros participantes comunicarán al Consejo de Administración, a más tardar el 31 de enero de cada año, el valor de las contribuciones a que se refiere el apartado 1 realizadas en cada uno de los ejercicios anteriores.

Artículo 23

Gastos y recursos del Centro de Competencia

1. El Centro de Competencia será financiado conjuntamente por la Unión y los Estados miembros mediante contribuciones financieras pagadas a plazos y contribuciones consistentes en los gastos realizados por los centros nacionales de coordinación y los beneficiarios al ejecutar acciones que no sean reembolsadas por el Centro de Competencia.

2. Los gastos administrativos del Centro de Competencia no excederán de [número] EUR y se sufragarán mediante contribuciones financieras divididas a partes iguales cada año entre la Unión y los Estados miembros participantes. Si una parte de la contribución destinada a sufragar los gastos administrativos no se utiliza, podrá destinarse a cubrir los gastos de funcionamiento del Centro de Competencia.

3. Los gastos de funcionamiento del Centro de Competencia se sufragarán por medio de:

   a) la contribución financiera de la Unión;

   b) contribuciones de los Estados miembros participantes en forma de:

      i) contribuciones financieras; y

      ii) cuando proceda, contribuciones en especie de los Estados miembros participantes consistentes en los gastos en que hayan incurrido los

centros nacionales de coordinación y los beneficiarios al ejecutar las acciones indirectas, deducida la contribución del Centro de Competencia y cualquier otra contribución de la Unión a dichos gastos.

4. Los recursos del Centro de Competencia consignados en su presupuesto se compondrán de:

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

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

   c) los ingresos generados por el Centro de Competencia;

   d) los demás recursos, ingresos y contribuciones financieras.

5. Los intereses devengados por las contribuciones aportadas al Centro de Competencia por los Estados miembros participantes serán considerados ingresos.

6. Todos los recursos del Centro de Competencia y sus actividades tendrán como fin lograr los objetivos establecidos en el artículo 4.

7. El Centro de Competencia será propietario de todos los activos que genere o que le sean transferidos para la consecución de sus objetivos.

8. Salvo en caso de liquidación del Centro de Competencia, los excedentes de ingresos sobre gastos no se abonarán a los miembros participantes del Centro de Competencia.

Artículo 24

Compromisos financieros

Los compromisos financieros del Centro de Competencia no excederán del importe de los recursos financieros disponibles o comprometidos en su presupuesto por sus miembros.

Artículo 25

Ejercicio presupuestario

El ejercicio presupuestario comenzará el 1 de enero y finalizará el 31 de diciembre.

Artículo 26

Establecimiento del presupuesto

1. El director ejecutivo elaborará cada año un proyecto de estado de previsiones de ingresos y gastos del Centro de Competencia para el siguiente ejercicio presupuestario, y lo transmitirá al Consejo de Administración junto con un proyecto de plantilla de personal. Deberá haber un equilibrio entre ingresos y gastos. El gasto del Centro de Competencia comprenderá los gastos de personal, los gastos administrativos, los gastos de infraestructura y los gastos de funcionamiento. Los gastos administrativos se limitarán al mínimo necesario.

2. El Consejo de Administración, sobre la base del proyecto de estado de previsiones de ingresos y gastos a que se refiere el apartado 1, presentará cada año la previsión de ingresos y gastos del Centro de Competencia para el siguiente ejercicio presupuestario.

3. El Consejo de Administración, a más tardar el 31 de enero de cada año, transmitirá a la Comisión el estado de previsiones a que se refiere el apartado 2, que formará parte del proyecto de documento único de programación.

4. Sobre la base de dicho estado de previsiones, la Comisión consignará en el proyecto de presupuesto de la Unión las previsiones que considere necesarias para la plantilla y el importe de la contribución que se imputará al presupuesto general, que deberá presentar al Parlamento Europeo y al Consejo de conformidad con los artículos 313 y 314 del TFUE.

5. El Parlamento Europeo y el Consejo autorizarán los créditos necesarios para la contribución destinada al Centro de Competencia.

6. El Parlamento Europeo y el Consejo aprobarán la plantilla del Centro de Competencia.

7. Junto con el plan de trabajo, el Consejo de Administración adoptará el presupuesto del Centro. Este se convertirá en definitivo tras la adopción final del presupuesto general de la Unión. Cuando proceda, el Consejo de Administración reajustará el presupuesto y el plan de trabajo del Centro de Competencia de conformidad con el presupuesto general de la Unión.

Artículo 27

Presentación de las cuentas y aprobación de la gestión del Centro de Competencia

La presentación de las cuentas provisionales y definitivas del Centro de Competencia y la aprobación de la gestión se ajustarán a las normas y al calendario del Reglamento Financiero y de las normas financieras del Centro adoptadas de conformidad con el artículo 29.

Artículo 28

Informes sobre funcionamiento y financieros

1. El director ejecutivo presentará anualmente al Consejo de Administración un informe sobre el desempeño de sus funciones, de conformidad con las normas financieras del Centro de Competencia.

2. En un plazo de dos meses tras el cierre de cada ejercicio financiero, el director ejecutivo presentará al Consejo de Administración, para su aprobación, un informe anual de actividades sobre los avances realizados por el Centro de Competencia durante el año natural anterior, en particular en relación con el plan de trabajo de dicho año. El informe incluirá, entre otras cosas, información sobre los asuntos siguientes:

   a) las actividades operativas realizadas y el gasto correspondiente;

   b) las acciones presentadas, junto con un desglose por tipo de participante, incluidas las pymes, y por Estado miembro;

   c) las acciones seleccionadas para su financiación, desglosadas por tipo de participante, incluidas las pymes, y por Estado miembro, con indicación de la contribución del Centro de Competencia para cada participante y cada acción;

   d) los avances en pos de la consecución de los objetivos establecidos en el artículo 4 y las propuestas respecto a la labor adicional que se necesita para lograr dichos objetivos.

3. Una vez aprobado por el Consejo de Administración, el informe anual de actividades se hará público.

Artículo 29

Normas financieras

El Centro de Competencia adoptará sus normas financieras específicas de conformidad con el artículo 70 del Reglamento XXX [nuevo Reglamento Financiero].

Artículo 30

Protección de los intereses financieros

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.

2. El Centro de Competencia permitirá al personal de la Comisión y a otras personas autorizadas por esta, así como al Tribunal de Cuentas, acceder a sus sedes y locales, así como a toda la información, incluida la información en formato electrónico, necesaria para llevar a cabo sus auditorías.

3. La Oficina Europea de Lucha contra el Fraude (OLAF) podrá llevar a cabo investigaciones, incluidos controles e inspecciones sobre el terreno, de conformidad con las disposiciones y procedimientos establecidos en el Reglamento (Euratom, CE) n.º 2185/96 del Consejo[30] y en el Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo[31], con el fin de determinar si ha habido fraude, corrupción o cualquier otra actividad ilegal que afecte a los intereses financieros de la Unión en relación con un acuerdo de subvención o un contrato financiado, directa o indirectamente, de conformidad con el presente Reglamento.

4. Sin perjuicio de lo dispuesto en los apartados 1, 2 y 3 del presente artículo, los contratos y acuerdos de subvención resultantes de la aplicación del presente Reglamento contendrán disposiciones que faculten expresamente a la Comisión, al Centro de Competencia, al Tribunal de Cuentas y a la OLAF a realizar dichas auditorías e investigaciones de conformidad con sus respectivas competencias. Cuando la ejecución de una acción se externalice o subdelegue, en su totalidad o en parte, o cuando exija la adjudicación de un contrato público o de ayuda financiera a terceros, el contrato o el acuerdo de subvención deberá incluir la obligación del contratista o del beneficiario de exigir a cualquier tercero que intervenga la

[30] Reglamento (Euratom, CE) n.º 2185/96 del Consejo, de 11 de noviembre de 1996, relativo a los controles y verificaciones *in situ* que realiza la Comisión para la protección de los intereses financieros de las Comunidades Europeas contra los fraudes e irregularidades (DO L 292 de 15.11.1996, p. 2).

[31] Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) y por el que se deroga el Reglamento (CE) n.º 1073/1999 del Parlamento Europeo y del Consejo y el Reglamento (Euratom) n.º 1074/1999 del Consejo (DO L 248 de 18.9.2013, p. 1).

aceptación explícita de las mencionadas competencias de la Comisión, del Centro de Competencia, del Tribunal de Cuentas y de la OLAF.

CAPÍTULO IV

PERSONAL DEL CENTRO DE COMPETENCIA

Artículo 31

Personal

1. Se aplicará al personal del Centro de Competencia el Estatuto de los funcionarios y el régimen aplicable a los otros agentes de la Unión Europea establecido por el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo[32] («Estatuto de los funcionarios» y «régimen aplicable a los otros agentes»), así como las normas adoptadas conjuntamente por las instituciones de la Unión con vistas a aplicar el Estatuto de los funcionarios y el régimen aplicable a los otros agentes.

2. El Consejo de Administración ejercerá, con respecto al personal del Centro de Competencia, las competencias atribuidas por el Estatuto de los funcionarios a la autoridad facultada para proceder a los nombramientos y las competencias atribuidas por el régimen aplicable a los otros agentes a la autoridad facultada para celebrar contratos («competencias de la autoridad facultada para proceder a los nombramientos»).

3. El Consejo de Administración adoptará, de conformidad con el artículo 110 del Estatuto de los funcionarios, una decisión basada en el artículo 2, apartado 1, del Estatuto de los funcionarios y en el artículo 6 del régimen aplicable a los otros agentes para delegar en el director ejecutivo las competencias correspondientes de la autoridad facultada para proceder a los nombramientos y determinar las condiciones en que podrá suspenderse la delegación de dichas competencias. El director ejecutivo podrá, a su vez, delegar tales competencias.

4. Cuando así lo exijan circunstancias excepcionales, el Consejo de Administración podrá, mediante resolución, suspender temporalmente la delegación en el director ejecutivo de las competencias de la autoridad facultada para proceder a los nombramientos y toda subdelegación realizada por este. En ese caso, el propio Consejo de Administración ejercerá las competencias de la autoridad facultada para proceder a los nombramientos o las delegará en uno de sus miembros o en un miembro del personal del Centro de Competencia distinto del director ejecutivo.

5. El Consejo de Administración adoptará normas de desarrollo respecto al Estatuto de los funcionarios y al régimen aplicable a los otros agentes, de conformidad con el artículo 110 del Estatuto de los funcionarios.

6. Los recursos de personal se determinarán en la plantilla de personal del Centro de Competencia, en la que se indicará el número de puestos temporales por grupo de función y grado, así como el número de personas contratadas, expresado en equivalentes a jornada completa, de conformidad con su presupuesto anual.

---

32 Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (DO L 56 de 4.3.1968, p. 1).

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

8. Todos los gastos de personal correrán a cargo del Centro de Competencia.

Artículo 32

Expertos nacionales en comisión de servicios y otros agentes

1. El Centro de Competencia podrá recurrir a expertos nacionales en comisión de servicios o a otro personal no contratado por el Centro de Competencia.

2. El Consejo de Administración adoptará una decisión por la que se establecerán las normas aplicables a los expertos nacionales en comisión de servicios en el Centro de Competencia, de acuerdo con la Comisión.

Artículo 33

Privilegios e inmunidades

El Protocolo n.º 7 sobre los privilegios y las inmunidades de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, será aplicable al Centro de Competencia y a su personal.

CAPÍTULO V

DISPOSICIONES COMUNES

Artículo 34

Normas de seguridad

1. El artículo 12, apartado 7, del Reglamento (UE) n.º XXX [programa Europa Digital] se aplicará a la participación en todas las acciones financiadas por el Centro de Competencia.

2. Las siguientes normas de seguridad específicas se aplicarán a las acciones financiadas con cargo a Horizonte Europa:

   a) a los efectos del artículo 34, apartado 1 [Propiedad y protección], del Reglamento (UE) n.º XXX [Horizonte Europa], cuando así lo disponga el plan de trabajo, la concesión de licencias no exclusivas podrá limitarse a terceros establecidos o que se considere que están establecidos en Estados miembros y controlados por Estados miembros o nacionales de Estados miembros;

   b) a efectos de lo dispuesto en el artículo 36, apartado 4, letra b) [Transferencia y concesión de licencias], del Reglamento (UE) n.º XXX [Horizonte Europa], la transferencia o concesión de una licencia a una entidad jurídica establecida en un país asociado o establecida en la Unión pero controlada por terceros países será también motivo para oponerse a la transferencia de la propiedad de los resultados o a la concesión de una licencia exclusiva sobre los resultados;

   c) a los efectos del artículo 37, apartado 3, letra a) [Derechos de acceso], del Reglamento (UE) n.º XXX [Horizonte Europa], cuando así lo disponga el plan de trabajo, la concesión de acceso a los resultados y a los conocimientos previos podrá limitarse solo a las entidades jurídicas establecidas o que se

considere que están establecidas en Estados miembros y controladas por Estados miembros o nacionales de Estados miembros.

Artículo 35

Transparencia

1. El Centro de Competencia realizará todas sus actividades con un alto grado de transparencia.
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.
3. El Consejo de Administración, a propuesta del director ejecutivo, podrá autorizar a las partes interesadas a participar en calidad de observadores en algunas de las actividades del Centro de Competencia.
4. El Centro de Competencia establecerá en su reglamento interno las disposiciones prácticas a efectos de la aplicación de las normas de transparencia a que se refieren los apartados 1 y 2. En el caso de las acciones financiadas con cargo a Horizonte Europa, se tendrán debidamente en cuenta las disposiciones del anexo III del Reglamento relativo a Horizonte Europa.

Artículo 36

Normas de seguridad sobre la protección de la información clasificada y de la información delicada no clasificada

1. Sin perjuicio de lo dispuesto en el artículo 35, el Centro de Competencia no divulgará a terceros la información que trate o reciba respecto de la que se haya presentado una solicitud motivada de tratamiento confidencial referida a la totalidad o a parte de la información.
2. Los miembros del Consejo de Administración, el director ejecutivo, los miembros del Consejo Consultivo Industrial y Científico, los expertos externos que participen en los grupos de trabajo *ad hoc* y los miembros del personal del Centro respetarán la obligación de confidencialidad en virtud del artículo 339 del Tratado de Funcionamiento de la Unión Europea, incluso después de haber cesado en sus cargos.
3. El Consejo de Administración del Centro de Competencia adoptará las normas de seguridad del Centro de Competencia, previa aprobación por la Comisión, sobre la base de los principios y normas establecidos en las normas de seguridad de la Comisión para la protección de la información clasificada de la Unión Europea (ICUE) y de la información delicada no clasificada, incluidas, entre otras disposiciones, las relativas al tratamiento y almacenamiento de dicha información establecidas en las Decisiones (UE, Euratom) 2015/443[33] y 2015/444[34] de la Comisión.

[33] Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (DO L 72 de 17.3.2015, p. 41).

4. El Centro de Competencia podrá adoptar todas las medidas necesarias para facilitar el intercambio de información pertinente para la ejecución de sus funciones con la Comisión y los Estados miembros, y, cuando proceda, con los órganos y organismos de la Unión competentes. Todo acuerdo administrativo celebrado a tal fin sobre el intercambio de ICUE o, cuando no exista dicho acuerdo, toda cesión *ad hoc* y con carácter excepcional de ICUE, deberá haber recibido previamente la aprobación de la Comisión.

Artículo 37

Acceso a los documentos

1. El Reglamento (CE) n.º 1049/2001 se aplicará a los documentos que obren en poder del Centro de Competencia.

2. El Consejo de Administración adoptará las disposiciones para la aplicación del Reglamento (CE) n.º 1049/2001 en el plazo de seis meses desde el establecimiento del Centro de Competencia.

3. Las decisiones adoptadas por el Centro de Competencia con arreglo al artículo 8 del Reglamento (CE) n.º 1049/2001 podrán ser objeto de una reclamación ante el Defensor del Pueblo Europeo de conformidad con el artículo 228 del Tratado de Funcionamiento de la Unión Europea o de un recurso ante el Tribunal de Justicia de la Unión Europea de conformidad con el artículo 263 del Tratado de Funcionamiento de la Unión Europea.

Artículo 38

Seguimiento, evaluación y revisión

1. El Centro de Competencia garantizará que sus actividades, incluidas las gestionadas a través de los centros nacionales de coordinación y de la Red, sean objeto de un seguimiento continuo y sistemático y de una evaluación periódica. El Centro de Competencia se asegurará de que los datos para el seguimiento de la ejecución y los resultados de los programas se recopilen de manera eficiente, eficaz y oportuna y que se impongan a los beneficiarios de los fondos de la Unión y a los Estados miembros unos requisitos de información proporcionados. Los resultados de la evaluación se harán públicos.

2. Una vez que se disponga de información suficiente sobre la aplicación del presente Reglamento, y a más tardar tres años y medio después del inicio de su aplicación, la Comisión llevará a cabo una evaluación intermedia del Centro de Competencia. La Comisión elaborará un informe sobre dicha evaluación y lo presentará al Parlamento Europeo y al Consejo a más tardar el 31 de diciembre de 2024. El Centro de Competencia y los Estados miembros proporcionarán a la Comisión la información necesaria para elaborar el informe.

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

[34] Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

que le han sido asignados, podrá proponer que se amplíe la duración del mandato del Centro de Competencia establecida en el artículo 46.

4. A partir de las conclusiones de la evaluación intermedia contemplada en el apartado 2, la Comisión podrá actuar de conformidad con el [artículo 22, apartado 5] o adoptar cualquier otra medida adecuada.

5. El seguimiento, la evaluación, la supresión progresiva y la renovación de la contribución con cargo a Horizonte Europa se regirán por lo dispuesto en los artículos 8, 45 y 47 y en el anexo III del Reglamento relativo a Horizonte Europa, así como por las modalidades de aplicación acordadas.

6. El seguimiento, la presentación de informes y la evaluación de la contribución con cargo a Europa Digital se regirán por lo dispuesto en los artículos 24 y 25 del programa Europa Digital.

7. En caso de liquidación del Centro de Competencia, la Comisión llevará a cabo una evaluación final de este en el plazo de seis meses desde la fecha de la liquidación y, en todo caso, dos años después de iniciarse el procedimiento de liquidación contemplado en el artículo 46 del presente Reglamento. Los resultados de la evaluación final se presentarán al Parlamento Europeo y al Consejo.

Artículo 39

Responsabilidad del Centro de Competencia

1. La responsabilidad contractual del Centro de Competencia se regirá por la legislación aplicable al acuerdo, la decisión o el contrato de que se trate.

2. En caso de responsabilidad extracontractual, el Centro de Competencia deberá reparar los daños causados por su personal en el ejercicio de sus funciones, de conformidad con los principios generales comunes a las legislaciones de los Estados miembros.

3. Cualquier pago por parte del Centro de Competencia en relación con la responsabilidad a que se refieren los apartados 1 y 2, así como los costes y gastos correspondientes, se considerarán gastos del Centro de Competencia y se cubrirán con sus recursos.

4. El Centro de Competencia será el único responsable del cumplimiento de sus obligaciones.

Artículo 40

Competencia del Tribunal de Justicia de la Unión Europea y Derecho aplicable

1. El Tribunal de Justicia de la Unión Europea será competente en lo siguiente:

   1) en relación con cualquier cláusula de arbitraje contenida en los acuerdos o contratos celebrados por el Centro de Competencia o en sus decisiones;

   2) en los litigios relativos a la indemnización por los daños causados por el personal del Centro de Competencia en el ejercicio de sus funciones;

3) en los litigios entre el Centro de Competencia y su personal, dentro de los límites y en las condiciones que se establecen en el Estatuto de los funcionarios.

2. Respecto de cualquier asunto que no esté contemplado en el presente Reglamento o en otros actos jurídicos de la Unión, se aplicará el Derecho del Estado miembro en que se ubique la sede del Centro de Competencia.

Artículo 41

Responsabilidad de los miembros y seguros

1. La responsabilidad financiera de los miembros respecto de las deudas del Centro de Competencia quedará limitada a las aportaciones que ya hayan efectuado para sufragar los gastos administrativos.

2. El Centro de Competencia suscribirá y mantendrá los seguros adecuados.

Artículo 42

Conflictos de intereses

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].

Artículo 43

Protección de los datos personales

1. 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.

2. El Consejo de Administración adoptará las normas de desarrollo a que se refiere el artículo xx, apartado 3, del Reglamento (UE) n.º xxx/2018. El Consejo de Administración podrá adoptar otras medidas necesarias para la aplicación del Reglamento (UE) n.º xxx/2018 por parte del Centro de Competencia.

Artículo 44

Apoyo del Estado miembro anfitrión

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.

CAPÍTULO VII

DISPOSICIONES FINALES

Artículo 45

Medidas iniciales

1. La Comisión será responsable del establecimiento y el funcionamiento inicial del Centro de Competencia hasta que este adquiera la capacidad funcional necesaria para ejecutar su propio presupuesto. La Comisión adoptará, de conformidad con el Derecho de la Unión, todas las medidas necesarias con la participación de los órganos competentes del Centro de Competencia.

2. A efectos del apartado 1, hasta que el director ejecutivo asuma sus funciones tras su nombramiento por el Consejo de Administración con arreglo al artículo 16, la Comisión podrá nombrar a un director ejecutivo interino para que ejerza las funciones asignadas al director ejecutivo, el cual podrá contar con la asistencia de un número limitado de funcionarios de la Comisión. La Comisión podrá destinar, con carácter provisional, a un número limitado de sus funcionarios.

3. El director ejecutivo interino podrá autorizar todos los pagos incluidos en los créditos que establezca el presupuesto anual del Centro de Competencia, una vez que hayan sido aprobados por el Consejo de Administración, y podrá adoptar decisiones y celebrar acuerdos y contratos, incluidos los contratos del personal, una vez aprobada la plantilla del Centro de Competencia.

4. El director ejecutivo interino determinará, de común acuerdo con el director ejecutivo del Centro de Competencia y previa aprobación del Consejo de Administración, la fecha en que el Centro de Competencia estará en condiciones de ejecutar su propio presupuesto. A partir de esa fecha, la Comisión dejará de asumir compromisos y realizar pagos en relación con las actividades del Centro de Competencia.

Artículo 46

Duración

1. El Centro de Competencia se establecerá para el período comprendido entre el 1 de enero de 2021 y el 31 de diciembre de 2029.

2. Al final de este período, a menos que se decida lo contrario mediante una revisión del presente Reglamento, se iniciará el procedimiento de liquidación. El procedimiento de liquidación se iniciará automáticamente si la Unión o todos los Estados miembros participantes se retiran del Centro de Competencia.

3. A fin de llevar a cabo el procedimiento de liquidación del Centro de Competencia, el Consejo de Administración nombrará a uno o varios liquidadores, que cumplirán sus decisiones.

4. En caso de liquidación, los activos del Centro de Competencia se utilizarán para cubrir sus pasivos y los gastos derivados de la liquidación. En caso de haber superávit, se distribuirá entre la Unión y los Estados miembros participantes de

manera proporcional a su contribución financiera al Centro de Competencia. El excedente que reciba la Unión se restituirá al presupuesto de esta.

Artículo 47

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA

1.3. Naturaleza de la propuesta/iniciativa

1.4. Objetivo(s)

1.5. Justificación de la propuesta/iniciativa

1.6. Duración e incidencia financiera

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema de gestión y de control

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

3.2.2. Incidencia estimada en los créditos de operaciones

3.2.3. Incidencia estimada en los créditos de carácter administrativo

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Reglamento por el que se establece el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA[35]

Investigación e innovación

Inversiones estratégicas europeas

1.3. Naturaleza de la propuesta/iniciativa

☒La propuesta/iniciativa se refiere a **una acción nueva**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[36]

☐ La propuesta/iniciativa se refiere a **la prolongación de una acción existente**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa

1. Un mercado único digital conectado

2. Un nuevo impulso al empleo, el crecimiento y la inversión

1.4.2. Objetivo(s) específico(s) de que se trate

Objetivos específicos

1.3. La economía digital puede desarrollar todo su potencial si se sustenta en iniciativas que permitan el pleno crecimiento de las tecnologías digitales y de datos.

2.1. Europa mantiene su posición de líder mundial en la economía digital, en la que las empresas europeas pueden crecer a escala mundial gracias a un fuerte espíritu empresarial digital y a la existencia de empresas emergentes competitivas, y en la que la industria y los servicios públicos dominan la transformación digital.

2.2. La investigación europea encuentra oportunidades de inversión para posibles avances tecnológicos y proyectos emblemáticos, en particular el programa Horizonte 2020/Horizonte Europa y la utilización de asociaciones público-privadas.

[35] GPA: Gestión por actividades. PPA: Presupuestación por actividades.

[36] Tal como se contempla en el artículo 54, apartado 2, letras a) o b), del Reglamento Financiero.

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

El Centro de Competencia, en colaboración con la Red y la Comunidad, tratará de alcanzar los siguientes objetivos:

1) contribuir a la ejecución de la parte relativa a la ciberseguridad del programa Europa Digital, establecido por el Reglamento n.º XXX, 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, y en particular la sección 2.2.6 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», y de otros programas de la Unión cuando así lo prevean los actos jurídicos de la Unión;

2) mejorar las capacidades, los conocimientos y las infraestructuras en materia de ciberseguridad al servicio de la industria, el sector público y la comunidad investigadora;

3) contribuir a una amplia implantación de los productos y las soluciones de ciberseguridad de última generación en todos los sectores de la economía;

4) mejorar la comprensión de la ciberseguridad y contribuir a reducir el déficit de capacidades en la Unión en relación con la ciberseguridad;

5) contribuir a reforzar la investigación y el desarrollo en materia de ciberseguridad en la Unión;

6) reforzar la colaboración entre las esferas civil y militar en lo que se refiere a las tecnologías y aplicaciones de doble uso;

7) reforzar las sinergias entre las dimensiones civil y militar de la ciberseguridad;

8) 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 10 y de la Comunidad de Competencias en Ciberseguridad a que se refiere el artículo 12.

1.4.4. Indicadores de resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

· Número de infraestructuras o herramientas de ciberseguridad contratadas conjuntamente.

· Acceso a tiempo de ensayo y experimentación puesto a disposición de los investigadores y la industria europeos en toda la Red y en el Centro. Si se trata de instalaciones ya existentes, el incremento del número de horas disponibles para dichas comunidades con respecto a las horas disponibles en la actualidad.

· El número de comunidades de usuarios a que se presta servicio y el número de investigadores que obtienen acceso a las instalaciones europeas de ciberseguridad aumenta con respecto al número de quienes tienen que buscar estos recursos fuera de Europa.

· Empieza a aumentar la competitividad de los proveedores europeos medida desde el punto de vista de la cuota de mercado mundial (objetivo de cuota de

mercado del 25 % de aquí a 2027) y desde el punto de vista de la proporción de resultados de la I+D europea asimilados por la industria.

· Contribución a las próximas tecnologías de ciberseguridad medida desde el punto de vista de derechos de autor, patentes, publicaciones científicas y productos comerciales.

· Número de planes de estudios relacionados con capacidades en materia de ciberseguridad evaluados y armonizados, y número de programas de certificación profesional en materia de ciberseguridad evaluados.

· Número de científicos, estudiantes y usuarios (usuarios industriales y administraciones públicas) formados.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

Conseguir una masa crítica de inversión en desarrollo tecnológico e industrial en relación con la ciberseguridad y superar la fragmentación de las capacidades correspondientes repartidas por toda la UE.

1.5.2. Valor añadido de la intervención de la UE

La ciberseguridad es una cuestión de interés común para la Unión, tal y como lo confirman las Conclusiones del Consejo mencionadas anteriormente. Es preciso tener en cuenta la magnitud y el carácter transfronterizo de incidentes como los de WannaCry o NonPetya. La naturaleza y la magnitud de los retos tecnológicos en materia de ciberseguridad, así como la insuficiente coordinación de los esfuerzos tanto dentro de la industria, el sector público y la comunidad investigadora como entre estas partes, exigen que la UE apoye en mayor medida los esfuerzos de coordinación a fin de poner en común una masa crítica de recursos y garantizar una mejor gestión de los conocimientos y los activos. Esto es necesario en vista de las exigencias de recursos en relación con determinadas capacidades para la investigación, el desarrollo y la implantación de la ciberseguridad; la necesidad de proporcionar acceso a conocimientos prácticos e interdisciplinares sobre ciberseguridad en diferentes disciplinas (a menudo solo parcialmente disponibles a nivel nacional); la naturaleza mundial de las cadenas de valor industriales, y la actividad de los competidores mundiales que están presentes en todos los mercados.

Para ello se requieren recursos y conocimientos especializados a una escala que difícilmente puede ser igualada por la acción individual de ningún Estado miembro. Por ejemplo, una red paneuropea de comunicación cuántica podría requerir una inversión de la UE del orden de 900 millones EUR, en función de las inversiones de los Estados miembros (que deberán interconectarse o completarse) y de la medida en que la tecnología permita la reutilización de las infraestructuras existentes.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La evaluación intermedia de Horizonte 2020, entre otras, confirmó la importancia que sigue teniendo el apoyo de la UE a la I+D y a los retos sociales (entre ellos, el denominado «Sociedades seguras», a partir del que se financia la I+D en ciberseguridad). Al mismo tiempo, la evaluación confirma que el refuerzo del liderazgo industrial sigue siendo un reto y que aún hay una brecha en materia de innovación, ya que la UE está rezagada en lo que se refiere a la innovación radical creadora de mercado.

La evaluación intermedia del Mecanismo «Conectar Europa» (MCE) parece confirmar el valor añadido de la intervención de la UE más allá de la I+D, si bien la ciberseguridad en el marco del MCE tenía un enfoque (en la seguridad operativa) y una lógica de intervención algo diferentes. Por otra parte, la mayoría de los beneficiarios de las subvenciones del MCE relativas a la ciberseguridad –la comunidad de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT)– ha manifestado su deseo de contar con un programa de apoyo a medida en el próximo marco financiero plurianual (MFP).

La creación en 2016 de la asociación público-privada (APPc) sobre ciberseguridad en la UE supuso un primer paso firme que reunió a las comunidades de la investigación, la industria y el sector público con el objetivo de facilitar la investigación y la innovación en materia de ciberseguridad, y, dentro de los límites del marco financiero 2014-2020, se espera que produzca resultados positivos y más específicos en el ámbito de la investigación y la innovación. La APPc hizo posible que los socios industriales manifestaran su compromiso en cuanto al gasto individual en los ámbitos definidos en la agenda estratégica de investigación e innovación de la asociación.

1.5.4. Compatibilidad y posibles sinergias con otros instrumentos adecuados

La red de competencias en ciberseguridad y el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad servirán de apoyo adicional para las actuales disposiciones políticas del ámbito de la ciberseguridad, así como para sus agentes. El mandato del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad será complementario de los esfuerzos de la ENISA, aunque su enfoque es diferente y requiere un conjunto de capacidades diferente. Mientras que la ENISA tiene un papel de asesoramiento sobre investigación e innovación en materia de ciberseguridad en la UE, el mandato propuesto para el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad se centra ante todo en otras funciones cruciales para reforzar la resiliencia en el ámbito de la ciberseguridad en la UE. El Centro debe estimular el desarrollo y la implantación de la tecnología en el ámbito de la ciberseguridad y complementar los esfuerzos de creación de capacidades en este ámbito a nivel nacional y de la UE.

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, junto con la red de competencias en ciberseguridad, también trabajará para apoyar la investigación destinada a facilitar y acelerar los procesos de normalización y certificación, en particular los relacionados con los sistemas de certificación de la ciberseguridad en el sentido del Reglamento de Ciberseguridad.

El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad actuará como mecanismo único para la ejecución de dos programas europeos que apoyan la ciberseguridad (programa Europa Digital y Horizonte Europa) y mejorará la coherencia y las sinergias entre ellos.

La presente iniciativa permite complementar los esfuerzos de los Estados miembros al proporcionar a los responsables de las políticas educativas los recursos adecuados para mejorar la educación en materia de ciberseguridad (por ejemplo, mediante la elaboración de planes de estudios sobre ciberseguridad en los sistemas educativos civil y militar, pero también proporcionando recursos para la educación básica sobre ciberseguridad). Asimismo, contribuiría a la armonización y la evaluación continua

de los programas de certificación profesional en el ámbito de la ciberseguridad, todo lo cual resulta necesario para ayudar a colmar las lagunas de capacidades relativas a la ciberseguridad y facilitar el acceso de las industrias y otras comunidades a los especialistas en ciberseguridad. La armonización de la educación y las capacidades contribuirá al desarrollo en la UE de una mano de obra cualificada en relación con la ciberseguridad, un activo clave para las empresas de ciberseguridad, así como para otras industrias interesadas en la ciberseguridad.

1.6. Duración e incidencia financiera

☒ Propuesta/iniciativa de **duración limitada**

– ☒ Propuesta/iniciativa en vigor desde el 1 de enero de 2021 hasta el 31 de diciembre de 2029.

– ☒ Incidencia financiera desde 2021 hasta 2027 para los créditos de compromiso y desde 2021 hasta 2031 para los créditos de pago.

☐ Propuesta/iniciativa de **duración ilimitada**

– Ejecución: fase de puesta en marcha desde AAAA hasta AAAA

– y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[37]

☐ **Gestión directa** a cargo de la Comisión

– ☐ por sus servicios, incluido su personal en las Delegaciones de la Unión,

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

☒

Gestión indirecta mediante delegación de tareas de ejecución presupuestaria en:

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especifíquense);

– ☐el BEI y el Fondo Europeo de Inversiones;

– ☒ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

– ☐ organismos de Derecho público;

– ☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

– ☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

[37] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

El artículo 28 contiene disposiciones detalladas sobre el seguimiento y la presentación de informes.

2.2. Sistema de gestión y de control

2.2.1. Riesgo(s) definido(s)

A fin de mitigar los riesgos relacionados con el funcionamiento del Centro de Competencia tras su creación y los retrasos, la Comisión apoyará al Centro de Competencia durante esta etapa para garantizar la rápida contratación del personal clave y el establecimiento de un sistema de control interno eficiente y de procedimientos adecuados.

2.2.2. Información relativa al sistema de control interno establecido

El director ejecutivo será responsable de las operaciones y la gestión cotidiana del Centro de Competencia, y será su representante legal. El director deberá rendir cuentas ante el Consejo de Administración y le informará continuamente del desarrollo de las actividades del Centro de Competencia.

El Consejo de Administración asume la responsabilidad general de la orientación estratégica y las operaciones del Centro de Competencia, y supervisará la realización de sus actividades.

El Consejo de Administración adoptará las normas financieras aplicables al Centro de Competencia, previa consulta a la Comisión. Dichas normas no podrán desviarse de lo dispuesto en el Reglamento (UE) n.º 1271/2013, salvo si las exigencias específicas de funcionamiento del Centro de Competencia lo requieren y la Comisión lo autoriza previamente.

El auditor interno de la Comisión desempeñará respecto al Centro de Competencia las mismas funciones que respecto a la Comisión. El Tribunal de Cuentas tendrá la facultad de auditar, a partir de documentos y sobre el terreno, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido del Centro de Competencia fondos de la Unión.

2.2.3. Estimación de los costes y beneficios de los controles y evaluación del nivel de riesgo de error esperado

Costes y beneficios de los controles

El coste del control para el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad se divide en el coste de la supervisión por parte de la Comisión y el coste de los controles operativos por parte del órgano de ejecución.

El coste de los controles por parte del Centro de Competencia se estima en alrededor del 1,19 % de los créditos de pago operativos ejecutados por el Centro de Competencia.

El coste de la supervisión por parte de la Comisión se estima en el 1,20 % de los créditos de pago operativos ejecutados por el Centro de Competencia.

Suponiendo que las actividades fueran gestionadas íntegramente por la Comisión sin el apoyo del órgano de ejecución, el coste del control sería sustancialmente superior y podría situarse en torno al 7,7 % de los créditos de pago.

Los controles previstos tienen el objetivo de asegurar una supervisión fluida y eficaz de las entidades de ejecución por parte de la Comisión y mantener el grado de garantía necesario para la Comisión.

Los beneficios de los controles son los siguientes:

- Evitar la selección de propuestas deficientes o inadecuadas.
- Optimizar la planificación y el uso de los fondos de la UE para preservar el valor añadido de la UE.
- Garantizar la calidad de los acuerdos de subvención, evitar errores en la identificación de las entidades jurídicas, garantizar el cálculo correcto de las contribuciones de la UE y adoptar las garantías necesarias para conseguir un correcto funcionamiento de las subvenciones.
- Detectar costes no subvencionables en la fase de pago.
- Detectar errores que afecten a la legalidad y la regularidad de las operaciones en la fase de auditoría.

Nivel de error estimado

El objetivo es mantener la tasa de error residual por debajo del umbral del 2 % para el conjunto del programa, al mismo tiempo que se limita la carga de control para que los beneficiarios logren el equilibrio adecuado entre el objetivo de legalidad y regularidad y otros objetivos tales como el atractivo del programa, en particular para las pymes, y el coste de los controles.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

La OLAF podrá llevar a cabo investigaciones, incluidos controles y verificaciones sobre el terreno, de conformidad con las disposiciones y los procedimientos establecidos en el Reglamento n.º 883/2013 del Parlamento Europeo y del Consejo y el Reglamento (Euratom, CE) n.º 2185/9640 del Consejo, de 11 de noviembre de 1996, relativo a los controles y verificaciones *in situ* que realiza la Comisión para la protección de los intereses financieros de la Unión contra los fraudes e irregularidades, con el fin de determinar si ha habido fraude, corrupción o cualquier otra actividad ilegal que afecte a los intereses financieros de la Unión en relación con una subvención o un contrato financiado por el Centro de Competencia.

Los acuerdos, decisiones y contratos resultantes de la aplicación del presente Reglamento deberán contener disposiciones que faculten expresamente a la Comisión, al Centro de Competencia, al Tribunal de Cuentas y a la OLAF para llevar a cabo auditorías e investigaciones, de conformidad con sus respectivas competencias.

El Centro de Competencia velará por que se protejan debidamente los intereses financieros de sus miembros realizando o encargando los oportunos controles internos y externos.

El Centro de Competencia se adherirá al Acuerdo interinstitucional, de 25 de mayo de 1999, entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión de las Comunidades Europeas, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF). El Centro de Competencia adoptará las medidas necesarias para facilitar las investigaciones internas a cargo de la OLAF.

El Centro de Competencia adoptará una estrategia antifraude basada en un análisis del riesgo de fraude y en consideraciones de rentabilidad. Protegerá los intereses financieros de la Unión 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 los importes abonados indebidamente y, cuando proceda, mediante sanciones administrativas y financieras que sean eficaces, proporcionales y disuasorias.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica del marco financiero plurianual y nueva(s) línea(s) presupuestaria(s) de gastos propuesta(s)

- Nuevas líneas presupuestarias solicitadas

  En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias:

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[38]	de países de la AELC[39]	de países candidatos [40]	de terceros países	a efectos de lo dispuesto en el artículo [21, apartado 2, letra b)], del Reglamento Financiero
Rúbrica 1: Mercado único, innovación y economía digital	01 02 XX XX Horizonte Europa, Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad: gastos de apoyo 01 02 XX XX Horizonte Europa, Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad 02 06 01 XX Programa Europa Digital, Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad: gastos de apoyo 02 06 01 XX Europa Digital, Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad	CD	SÍ	SÍ (si aparece especificado en el programa de trabajo anual)	SÍ (limitado a algunas partes del programa)	NO

[38] CD = créditos disociados / CND = créditos no disociados.

[39] AELC: Asociación Europea de Libre Comercio.

[40] Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales

- Se espera que las contribuciones a esta línea presupuestaria procedan de:

En millones EUR (al tercer decimal)

Línea presupuestaria	Año 2021	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	**Total**
01 01 01 01 Gastos relativos a funcionarios y agentes temporales que se ocupan de la investigación: Horizonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Personal externo que ejecuta los programas de investigación: Horizonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Otros gastos de gestión de los programas de investigación: Horizonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Desafíos mundiales y competitividad industrial	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Apoyo administrativo: programa Europa Digital	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Ciberseguridad: programa Europa Digital	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Total de gastos	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

La contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), será propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político. La propuesta se basará en los resultados del proceso de planificación estratégica definido en el artículo 6, apartado 6, del Reglamento XXX [programa marco Horizonte Europa].

Estos importes no incluyen la contribución de los Estados miembros a los costes de funcionamiento y administrativos del Centro de Competencia, proporcional a la contribución financiera de la Unión.

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	**1**	Mercado único, innovación y economía digital

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Después de 2027***	**TOTAL**
Título 1 (Gastos de personal)	Compromisos = Pagos	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Título 2 (Infraestructura y gastos de funcionamiento)	Compromisos = Pagos	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Título 3 (Gastos operativos)	Compromisos	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Pagos	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTAL de los créditos de la dotación de	Compromisos	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] Los créditos de personal solo se contabilizan medio año en 2021

los programas[42]	Pagos	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] El total de créditos establecido solo se refiere a los recursos financieros de la UE destinados a la ciberseguridad en el marco de Europa Digital. La contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 5, apartado 1, letra b), será propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político. La propuesta se basará en los resultados del proceso de planificación estratégica definido en el artículo 6, apartado 6, del Reglamento XXX [programa marco Horizonte Europa].

Rúbrica del marco financiero plurianual	7	«Gastos administrativos»

En millones EUR (al tercer decimal)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Después de 2027***	**TOTAL**
Recursos humanos		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Otros gastos administrativos		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAL de los créditos para la RÚBRICA 7 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

En millones EUR (al tercer decimal)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Después de 2027***	**TOTAL**
TOTAL de los créditos de las distintas RÚBRICAS del marco financiero plurianual	Compromisos	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Pagos	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 061,715**	**2 005,637**

3.2.2. Resumen de la incidencia estimada en los créditos de carácter administrativo

– ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

– ☒ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

Años	2021	2022	2023	2024	2025	2026	2027	TOTAL
RÚBRICA 7 del marco financiero plurianual								
Recursos humanos	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Otros gastos administrativos	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotal para la RÚBRICA 7 del marco financiero plurianual	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Al margen de la RÚBRICA 7[43] del marco financiero plurianual								
Recursos humanos								
Otros gastos de carácter administrativo	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

TOTAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción y/o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Los créditos que se mencionan necesarios para recursos humanos y otros gastos de carácter administrativo al margen de la rúbrica 7 corresponden a los importes cubiertos por la contribución financiera de la Unión con cargo al programa Europa Digital.

A los créditos necesarios para recursos humanos y otros gastos de carácter administrativo al margen de la rúbrica 7 se sumarán los importes cubiertos por la contribución financiera de la Unión con cargo al programa Horizonte Europa, una vez

[43] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

que la contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), sea propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político.

Los importes mencionados de los créditos necesarios para recursos humanos y otros gastos de carácter administrativo al margen de la rúbrica 7 no incluyen la contribución de los Estados miembros a los costes administrativos del Centro de Competencia, proporcional a la contribución financiera de la Unión.

3.2.2.1. Necesidades estimadas de recursos humanos en la Comisión

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– ■ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

Años		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Empleos de plantilla (funcionarios y personal temporal)								
Sede y Oficinas de Representación de la Comisión		20	21	21	21	21	21	22
Delegaciones								
Investigación								
• Personal externo (en unidades de equivalente a jornada completa, EJC), AC, LA, ENCS, INT y JED [44] Rúbrica 7								
Financiado mediante la RÚBRICA 7 del marco financiero plurianual	- en la sede	3	3	3	3	3	3	3
	- en las Delegaciones							
Financiado mediante la dotación del programa [45]	- en la sede							
	- en las Delegaciones							
Investigación								
Otros (especifíquense)								
TOTAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Coordinación, supervisión y dirección de las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, incluidos los costes de apoyo y coordinación. Elaboración y coordinación de políticas en el ámbito de la ciberseguridad en relación con las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, por ejemplo, en lo que se refiere al establecimiento de prioridades para la investigación y la política industrial, la cooperación general entre los Estados miembros y los agentes económicos, la coherencia con el futuro marco de certificación de la ciberseguridad de la UE, la labor sobre responsabilidad y deber de asistencia, o la coordinación con las políticas en materia de informática de alto

44 AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JED = joven experto en delegación.

45 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

	rendimiento, inteligencia artificial y capacidades digitales. .
Personal externo	Coordinación, supervisión y dirección de las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, incluidos los costes de apoyo y coordinación. Elaboración y coordinación de políticas en el ámbito de la ciberseguridad en relación con las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, por ejemplo, en lo que se refiere al establecimiento de prioridades para la investigación y la política industrial, la cooperación general entre los Estados miembros y los agentes económicos, la coherencia con el futuro marco de certificación de la ciberseguridad de la UE, la labor sobre responsabilidad y deber de asistencia, o la coordinación con las políticas en materia de informática de alto rendimiento, inteligencia artificial y capacidades digitales. .

3.2.2.2. Necesidades estimadas de recursos humanos en el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad

	2021	2022	2023	2024	2025	2026	2027
Funcionarios de la Comisión							
De los cuales AD							
De los cuales AST							
De los cuales AST-SC							
Agentes temporales							
De los cuales AD	10	11	13	13	13	13	13
De los cuales AST							
De los cuales AST-SC							
Agentes contractuales	26	32	39	39	39	39	39
ENCS	1	1	1	1	1	1	1
Total	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Ejecución operativa de las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, con arreglo al artículo 4 del presente Reglamento, incluidos los costes de apoyo y coordinación.
Personal externo	Ejecución operativa de las funciones encomendadas al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, con arreglo al artículo 4 del presente Reglamento, incluidos los costes de apoyo y coordinación.

Las necesidades estimadas de recursos humanos en el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad antes mencionadas corresponden a las necesidades estimadas para ejecutar la contribución financiera de la Unión en el marco de Europa Digital.

A las necesidades estimadas de recursos humanos en el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad antes mencionadas se sumarán las necesidades estimadas para ejecutar la contribución financiera de la Unión en el marco de Horizonte Europa, una vez que la contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), sea propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político.

3.2.2.3. Plantilla de personal del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad

Categoría y grado	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Total AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
Total AST							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Total AST/SC							
TOTAL GENERAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Incidencia estimada en el personal (adicional), personal externo del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad

Agentes contractuales	2021	2022	2023	2024	2025	2026	2027
Grupo de funciones IV	20	22	29	29	29	29	29
Grupo de funciones III	2	4	4	4	4	4	4
Grupo de funciones II	4	6	6	6	6	6	6
Grupo de funciones I							
Total	**26**	**32**	**39**	**39**	**39**	**39**	**39**

A fin de garantizar la contención del aumento de efectivos, el aumento de personal del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad se compensará parcialmente reduciendo el número de funcionarios y de personal externo (es decir, la plantilla de personal y el personal externo existentes) en los servicios pertinentes de la Comisión.

La plantilla del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad que se indica en los puntos 3.2.2.2 a 4 se compensará del siguiente modo[46]:

TOTAL	2021	2022	2023	2024	2025	2026	2027
Funcionarios de la Comisión	5	5	6	6	6	6	6
Agentes temporales							
Agentes	14	17	20	20	20	20	20

[46] A reserva del importe definitivo del presupuesto cuya ejecución se delegará en el Centro de Competencia

contractuales							
ENCS							
Total EJC	19	22	26	26	26	26	26
Plantilla	19	22	26	26	26	26	26

La compensación de los recursos humanos del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad será proporcional a la parte de la contribución financiera de la Unión, es decir, el 50 %.

La compensación mencionada se refiere a las necesidades estimadas de recursos humanos en el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad para ejecutar la contribución financiera de la Unión con cargo a Europa Digital.

A la compensación mencionada se sumarán las necesidades estimadas para ejecutar la contribución financiera de la Unión con cargo a Horizonte Europa, una vez que la contribución de la dotación financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), sea propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político.

3.2.3. Contribución de terceros

La propuesta/iniciativa:

– ☐ no prevé la cofinanciación por terceros

– ☒ prevé la cofinanciación por terceros[47] que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

Años	2021	2022	2023	2024	2025	2026	2027	TOTAL
Estados miembros, contribución a los gastos de personal	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Estados miembros, contribución a los gastos de infraestructuras y funcionamiento	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Estados miembros, contribución a los gastos operativos	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTAL de los créditos cofinanciados	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

La contribución de terceros mencionada solo se refiere a la cofinanciación proporcional a los recursos financieros de la UE destinados a la ciberseguridad en el marco de Europa Digital. La contribución de terceros mencionada se aumentará una vez que la contribución financiera del clúster «Sociedad inclusiva y segura» del pilar II «Desafíos mundiales y competitividad industrial» de Horizonte Europa (dotación total: 2 800 millones EUR) a que se refiere el artículo 21, apartado 1, letra b), sea propuesta por la Comisión durante el proceso legislativo, y, en cualquier caso, antes de que se alcance un acuerdo político. La propuesta se basará en los resultados del proceso de planificación estratégica definido en el artículo 6, apartado 6, del Reglamento XXX [programa marco Horizonte Europa].

3.3. Incidencia estimada en los ingresos

– ☒ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

☐ en los recursos propios

☐ en ingresos diversos

indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de	Incidencia de la propuesta/iniciativa[48]

[47] Contribución en especie estimada de los Estados miembros

[48] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 20 % de los gastos de recaudación.

ingresos:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artículo …….							

En el caso de los ingresos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

Otras observaciones (por ejemplo, método/fórmula que se utiliza para calcular la incidencia sobre los ingresos o cualquier otra información).