

Bruselas, 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE

This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

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»)

(Texto pertinente a efectos del EEE)

{SWD(2017) 500 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La Unión Europea ha adoptado una serie de medidas para incrementar la resiliencia y mejorar su preparación en materia de ciberseguridad. La primera Estrategia de Ciberseguridad de la UE¹, adoptada en 2013, estableció objetivos estratégicos y acciones concretas para mejorar la resiliencia, reducir la ciberdelincuencia, desarrollar políticas y capacidades en materia de ciberdefensa, desarrollar recursos industriales y tecnológicos y establecer una política coherente del ciberespacio internacional para la UE. En este contexto, se han producido desde entonces acontecimientos importantes, en particular el segundo mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)² y la adopción de la **Directiva sobre seguridad de las redes y los sistemas de información**³ (en lo sucesivo, «Directiva SRI»), que constituyen la base de la presente propuesta.

Por otra parte, en 2016 la Comisión Europea adoptó la Comunicación «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora»⁴, en la que se anunciaron nuevas medidas para intensificar la cooperación, la información y la puesta en común de conocimientos y para incrementar la resiliencia y preparación de la UE, teniendo también en cuenta la perspectiva de incidentes a gran escala y una posible crisis paneuropea de ciberseguridad. En este contexto, la Comisión anunció que presentaría la **evaluación y revisión** del Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo relativo a ENISA y por el que se deroga el Reglamento (CE) n.º 460/2004 (el «Reglamento de ENISA»). El proceso de evaluación podría conducir a una posible reforma de la Agencia y a un reforzamiento de sus facultades y capacidades para apoyar a los Estados miembros de manera sostenible. Le conferiría, por tanto, un papel más operativo y central para lograr la resiliencia en materia de ciberseguridad y reconocería en su nuevo mandato las nuevas responsabilidades de la Agencia en virtud de la Directiva SRI.

La Directiva SRI representa un primer paso esencial con vistas a fomentar una cultura de gestión de riesgos, al introducir requisitos de seguridad como obligaciones legales de los agentes económicos clave, en particular los operadores que prestan servicios esenciales (operadores de servicios esenciales u OSE) y los proveedores de algunos servicios digitales clave (proveedores de servicios digitales o PSE). Dado que los requisitos de seguridad se consideran esenciales para salvaguardar los beneficios de la digitalización de la sociedad en curso, y vista la rápida proliferación de dispositivos conectados (la «internet de las cosas»), la Comunicación de 2016 también proponía la idea de crear un marco para la certificación de seguridad de los productos y servicios de TIC a fin de incrementar la confianza y la seguridad en el mercado único digital. La certificación de ciberseguridad de las TIC adquiere particular importancia teniendo en cuenta el creciente uso de tecnologías que requieren un elevado nivel

¹ Comunicación conjunta de la Comisión Europea y el Servicio Europeo de Acción Exterior: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», JOIN(2013).

² Reglamento (UE) n.º 526/2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004

³ Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

⁴ Comunicación de la Comisión «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora» (COM/2016/410 final).

de ciberseguridad, como los automóviles conectados y automatizados, la sanidad electrónica o los sistemas de control de automatización industrial (IACS).

Estas medidas y anuncios políticos quedaron aún más reforzados tras las **conclusiones del Consejo** de 2016, que reconocían que «las ciberamenazas y las vulnerabilidades siguen evolucionando e intensificándose, lo cual requerirá una cooperación continuada y más estrecha, sobre todo a la hora de dar respuesta a incidentes de ciberseguridad transfronterizos y de gran envergadura». Dichas conclusiones reafirmaban que «el Reglamento ENISA es uno de los elementos básicos del marco de la UE sobre ciberresiliencia»⁵ y pedían a la Comisión que tomase nuevas medidas para abordar la cuestión de la certificación a nivel europeo.

El establecimiento de un sistema de certificación exigiría la implantación de un sistema de gobernanza adecuado a nivel de la UE, entre otras cosas gracias a los conocimientos aportados por una agencia de la UE independiente. A este respecto, la presente propuesta señala a ENISA como el organismo natural a nivel de la UE competente para la ciberseguridad que debería asumir esa función para reunir a los organismos nacionales competentes en materia de certificación y coordinar su trabajo.

En su Comunicación sobre la **revisión intermedia de la Estrategia para el Mercado Único Digital de mayo de 2017**, la Comisión especificó además que, a más tardar en septiembre de 2017, revisaría el mandato de ENISA. Se trataría de definir su papel en el cambiante ecosistema de la ciberseguridad y de desarrollar medidas relativas a normas, certificación y etiquetado de ciberseguridad para aumentar la ciberseguridad de los sistemas basados en las TIC, incluidos los objetos conectados⁶. Las **conclusiones del Consejo Europeo** de junio de 2017⁷ saludaron la intención de la Comisión de revisar la estrategia de ciberseguridad en septiembre y de proponer nuevas acciones específicas antes de finalizar 2017.

La propuesta de Reglamento establece un conjunto completo de medidas que se basan en actuaciones anteriores y fomentan objetivos específicos que se refuerzan mutuamente:

- aumentar **las capacidades y la preparación** de los Estados miembros y de las empresas;
- mejorar **la cooperación y la coordinación** entre los Estados miembros y las instituciones, órganos y organismos de la UE;
- aumentar **las capacidades a nivel de la UE para complementar la acción de los Estados miembros**, en particular en caso de ciber crisis transfronteriza;
- aumentar **la sensibilización** de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad;
- aumentar en general **la transparencia de la garantía de ciberseguridad**⁸ de los productos y servicios de TIC, a fin de reforzar la confianza en el mercado único digital y en la innovación digital; y

⁵ Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

⁶ Comunicación de la Comisión relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, COM(2017) 228.

⁷ Reunión del Consejo Europeo (22 y 23 de junio de 2017): Conclusiones EUCO 8/17.

⁸ La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información suficiente sobre las propiedades de ciberseguridad para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

- evitar **la fragmentación de los sistemas de certificación** en la UE y de los requisitos de seguridad y criterios de evaluación conexos en los distintos Estados miembros y sectores.

La siguiente sección de la exposición de motivos explica con más detalle la justificación de la iniciativa con respecto a las acciones propuestas para ENISA y la certificación de ciberseguridad.

ENISA

ENISA actúa como centro de conocimientos especializados para mejorar la seguridad de las redes y de la información en la Unión y apoyar la creación de capacidades en los Estados miembros.

ENISA se creó en 2004⁹ con el fin de contribuir al objetivo general de garantizar un elevado nivel de seguridad de las redes y de la información en la UE. En 2013, el Reglamento (UE) n.º 526/2013 estableció el nuevo mandato de la Agencia para un período de siete años, hasta 2020. La Agencia tiene sus oficinas en Grecia, en particular con sede administrativa en Heraklion (Creta) y operaciones principales en Atenas.

ENISA es una agencia pequeña, cuyo presupuesto y efectivos son bajos en comparación con todas las agencias de la UE. Su mandato es de duración determinada.

ENISA asiste a las instituciones europeas, los Estados miembros y la comunidad empresarial a la hora de **abordar, dar respuesta y especialmente prevenir los problemas de seguridad de las redes y de la información**. Lo hace a través de una serie de actividades en los cinco ámbitos enunciados en su estrategia¹⁰:

- Asesoramiento: suministro de información y asesoramiento sobre las principales cuestiones de seguridad de las redes y de la información.
- Política: apoyo a la elaboración y aplicación de políticas en la Unión.
- Capacidad: apoyo a la creación de capacidad en la Unión (por ejemplo, mediante formación, recomendaciones y actividades de sensibilización).
- Comunidad: impulsar al colectivo de la seguridad de las redes y de la información (por ejemplo, apoyo a los equipos de respuesta a emergencias informáticas o CERT, o coordinación de ciberejercicios paneuropeos).
- Facilitación (por ejemplo, contactos con las partes interesadas y relaciones internacionales).

En el curso de las negociaciones de la Directiva SRI, los legisladores de la UE decidieron asignar importantes funciones a ENISA a la hora de aplicar dicha Directiva. En particular, la Agencia se encarga de la secretaría de la red de CSIRT (establecida para promover la cooperación operativa rápida y eficaz entre los Estados miembros sobre incidentes de ciberseguridad específicos y compartir información sobre riesgos), y también debe prestar asistencia al Grupo de cooperación en la ejecución de sus tareas. Además, la Directiva exige a

⁹ Reglamento (CE) n.º 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

¹⁰ <https://www.enisa.europa.eu/publications/corporate/enisa-strategy>

ENISA que preste asistencia a los Estados miembros y a la Comisión ofreciéndoles sus conocimientos y asesoramiento y facilitando el intercambio de las mejores prácticas.

De conformidad con el Reglamento de ENISA, la Comisión ha llevado a cabo una evaluación de la Agencia, que incluye un estudio independiente, así como una consulta pública. La evaluación se centró en la pertinencia, repercusión, eficacia, eficiencia, coherencia y valor añadido europeo de la Agencia en lo que se refiere a su rendimiento, gobernanza, estructura organizativa interna y prácticas de trabajo durante el período 2013-2016.

El rendimiento global de ENISA fue evaluado positivamente por la mayoría de quienes respondieron¹¹ (74 %) a la consulta pública. También fue mayoritaria la opinión de que ENISA estaba alcanzando sus diferentes objetivos (al menos un 63 % para cada uno de los objetivos). Los servicios y productos de ENISA son utilizados de forma regular (mensualmente o con mayor frecuencia) por casi la mitad de quienes respondieron (46 %) y apreciados por el hecho de proceder de un organismo a nivel de la UE (83 %) y por su calidad (62 %).

No obstante, una gran mayoría (88 %) de las respuestas consideraba que los actuales instrumentos y mecanismos disponibles a nivel de la UE son insuficientes o solo parcialmente adecuados para hacer frente a los actuales desafíos en materia de ciberseguridad. Una gran mayoría de las respuestas (98 %) indicaba que un organismo de la UE debía abordar estas necesidades y, entre ellos, al 99 % ENISA le parecía la organización adecuada para ello. Además, el 67,5 % de las respuestas expresó la opinión de que ENISA podría desempeñar algún papel en el establecimiento de un marco armonizado para la certificación de seguridad de los productos y servicios de TI.

La evaluación global (sobre la base no solo de la consulta pública, sino también de una serie de entrevistas personales, encuestas específicas adicionales y seminarios) llegó a las siguientes conclusiones:

- Los objetivos de ENISA siguen siendo pertinentes en la actualidad. En un contexto de rápida evolución tecnológica y de amenazas cambiantes, y visto que los riesgos globales relacionados con la ciberseguridad son cada vez mayores, existe una clara necesidad en la UE de fomentar y seguir reforzando los conocimientos técnicos de alto nivel sobre cuestiones de ciberseguridad. Deben crearse en los Estados miembros capacidades que permitan comprender y responder a las amenazas, y es precisa una cooperación de las partes interesadas en todos los ámbitos temáticos e instituciones.
- A pesar de su reducido presupuesto, la Agencia ha sido operativamente eficiente en la utilización de sus recursos y en el desempeño de sus funciones. La existencia de dos sedes en Atenas y Heraklion, no obstante, ha generado también costes administrativos suplementarios.
- En cuanto a eficacia, ENISA ha alcanzado parcialmente sus objetivos. La Agencia ha contribuido satisfactoriamente a la mejora de la seguridad de las redes y de la información en Europa merced a la oferta de creación de capacidad en 28 Estados

¹¹ Noventa partes interesadas procedentes de 19 Estados miembros respondieron a la consulta (88 respuestas y 2 documentos de posición), incluidas las autoridades nacionales de 15 Estados miembros y 8 organizaciones representativas de un número importante de empresas europeas.

miembros¹², mejorando la cooperación entre los Estados miembros y las partes interesadas de la seguridad de las redes y de la información y facilitando asesoramiento, creando comunidades y apoyando la formulación de políticas. Globalmente, ENISA se ha centrado diligentemente en la ejecución de su programa de trabajo y ha actuado como socio fiable de las partes interesadas, en un ámbito cuya acusada importancia transfronteriza ha sido reconocida solo recientemente.

- ENISA consiguió dejar su huella, al menos en cierta medida, en el amplio campo de la seguridad de las redes y de la información, pero no ha conseguido plenamente desarrollar una imagen sólida ni obtener visibilidad suficiente para ser reconocida como «el» centro de conocimientos especializados en Europa. La explicación reside en la amplitud de su mandato, que no iba acompañado de unos recursos proporcionalmente suficientes. Además, ENISA es la única agencia de la UE cuyo mandato es de duración determinada, lo que limita su capacidad para desarrollar una visión a largo plazo y apoyar a sus partes interesadas de manera sostenible. Esto contrasta también con las disposiciones de la Directiva SRI, que atribuye a ENISA tareas sin señalar fecha de finalización. Por último, la evaluación constató que esta limitada eficacia puede explicarse en parte por la fuerte dependencia de asesoramiento externo con preferencia al interno y por las dificultades para contratar y retener personal especializado.
- La última, pero no menos importante, conclusión de la evaluación es que el valor añadido de ENISA radica principalmente en su capacidad para potenciar la cooperación sobre todo entre los Estados miembros, y especialmente con los colectivos interesados en la seguridad de las redes y de la información (en particular entre los CSIRT). No existe nadie a nivel de la UE que preste apoyo a una gama tan amplia de partes interesadas en la seguridad de las redes y de la información. No obstante, debido a la necesidad de priorizar estrictamente sus actividades, el programa de trabajo de ENISA lo definen principalmente las necesidades de los Estados miembros. En consecuencia, no responde suficientemente a las de otras partes interesadas, en particular la industria. Además, esto hizo que la Agencia tratara de satisfacer las necesidades de sus interlocutores clave, lo que le impidió alcanzar un impacto mayor. Por lo tanto, el valor añadido aportado por la Agencia fue distinto según las necesidades divergentes de sus partes interesadas y la medida en que la Agencia pudo responder a ellas (por ejemplo, grandes frente a pequeños Estados miembros; Estados miembros frente a la industria).

En resumen, los resultados de las consultas con las partes interesadas y de la evaluación sugirieron la necesidad de adaptar los recursos y el mandato de ENISA para que pueda desempeñar un papel adecuado en la respuesta a los retos actuales y futuros.

¹² Se pidió a quienes respondieron a la consulta pública que indicaran cuáles consideraban los principales logros de ENISA durante el período 2013-2016. Respuestas procedentes de todos los grupos (55 en total, incluidas 13 de autoridades nacionales, 20 del sector privado y 22 de «otros») percibieron los siguientes logros principales de ENISA: 1) la coordinación de los ejercicios de Cyber Europe; 2) la prestación de apoyo a los CERT/CSIRT a través de cursos de formación y seminarios para fomentar la coordinación y el intercambio; 3) las publicaciones de ENISA (directrices y recomendaciones, informes sobre la perspectiva de amenazas, estrategias para la notificación de incidentes y la gestión de crisis, etc.) que se consideraron útiles tanto para crear y actualizar los marcos nacionales de seguridad como para servir de referencia a los responsables de la formulación de políticas y a los profesionales de la ciberseguridad; 4) la contribución a la promoción de la Directiva SRI; 5) los esfuerzos destinados a aumentar la sensibilización a través del mes de la ciberseguridad.

Habida cuenta de estos resultados, la presente propuesta revisa el actual mandato de ENISA y establece un nuevo conjunto de tareas y funciones, con vistas a apoyar de manera efectiva y eficaz los esfuerzos de los Estados miembros, las instituciones de la UE y otras partes interesadas para garantizar la seguridad del ciberespacio en la Unión Europea. El nuevo mandato propuesto pretende atribuir a la Agencia funciones más sólidas y centrales, en particular respaldando también a los Estados miembros a la hora de aplicar la Directiva SRI y hacer frente a amenazas específicas de manera más activa (capacidad operativa), y convirtiéndose en un centro de conocimientos especializados que asista a los Estados miembros y la Comisión en el ámbito de la certificación de la ciberseguridad. En virtud de la presente propuesta:

- ENISA recibiría un mandato permanente que le proporcionaría una base estable para el futuro. El mandato, los objetivos y las funciones deberían seguir sujetos a revisión periódica.
- El mandato propuesto aclara en mayor medida el papel de ENISA como agencia de la UE para la ciberseguridad y como punto de referencia en el ecosistema de ciberseguridad de la UE, actuando en estrecha cooperación con todos los demás organismos pertinentes de dicho ecosistema.
- La organización y la gobernanza de la Agencia, que se consideraron positivas en la evaluación, serían moderadamente revisadas, en particular para cerciorarse de que queden mejor reflejadas en su trabajo las necesidades de la comunidad de partes interesadas en general.
- Se delinea el alcance propuesto del mandato, que refuerza los ámbitos en los que la Agencia ha mostrado un claro valor añadido y añade otros nuevos en los que se necesita apoyo a la vista de los nuevos instrumentos y prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el inminente plan director de ciberseguridad de la UE para la cooperación en caso de ciber crisis y la certificación de seguridad de las TIC.
- **Formulación y ejecución de las políticas de la UE:** ENISA se encargaría de contribuir proactivamente a la elaboración de políticas en el ámbito de la seguridad de las redes y la información, así como a otras iniciativas políticas con elementos de ciberseguridad en los distintos sectores (como energía, transporte o finanzas). Para ello, debería poseer un sólido papel consultivo, que podría desempeñar aportando dictámenes independientes y trabajos preparatorios para el desarrollo y la actualización de las políticas y la legislación. ENISA también prestaría apoyo a las políticas y la legislación de la UE en el ámbito de las comunicaciones electrónicas, la identidad electrónica y los servicios de confianza, con vistas a promover un mayor nivel de ciberseguridad. En la fase de aplicación, en particular en el contexto del Grupo de cooperación de la SRI, ENISA asistiría a los Estados miembros en la consecución de un planteamiento coherente sobre la aplicación de la Directiva SRI a través de fronteras y sectores, así como en otras leyes y políticas pertinentes. A fin de sostener la revisión periódica de las políticas y la legislación en el ámbito de la ciberseguridad, ENISA proporcionaría también informes periódicos sobre el estado de la aplicación del marco jurídico de la UE.
- **Creación de capacidades:** ENISA contribuiría a la mejora de las capacidades y conocimientos técnicos de las autoridades públicas nacionales y de la UE, en particular en lo que se refiere a la respuesta a incidentes y a la supervisión de

las medidas reglamentarias relacionadas con la ciberseguridad. La Agencia también debería contribuir al establecimiento de los centros de puesta en común y análisis de la información (ISACS) en diversos sectores, aportando mejores prácticas y orientaciones sobre los procedimientos e instrumentos disponibles, así como abordando adecuadamente las cuestiones reglamentarias relacionadas con el intercambio de información.

- **Conocimientos e información, sensibilización:** ENISA se convertiría en la plataforma de información de la UE. Esto implicaría la promoción y el intercambio de las mejores prácticas e iniciativas en toda la UE mediante la puesta en común de información sobre ciberseguridad procedente de las instituciones, órganos y organismos nacionales y de la UE. La Agencia facilitaría asimismo asesoramiento, orientación y mejores prácticas sobre la seguridad de las infraestructuras críticas. Tras un incidente transfronterizo de ciberseguridad importante, ENISA elaboraría también informes con el fin de ofrecer orientaciones a las empresas y los ciudadanos de toda la UE. Esta línea de trabajo implicaría también la organización periódica de actividades de sensibilización, en coordinación con las autoridades de los Estados miembros.
- **Tareas relacionadas con el mercado (normalización, certificación de la ciberseguridad):** ENISA desempeñaría una serie de funciones específicas de apoyo del mercado interior, incluido un «observatorio del mercado» de la ciberseguridad, analizando las tendencias pertinentes en el mercado de la ciberseguridad para adecuar mejor la oferta y la demanda, y respaldando el desarrollo de las políticas de la UE en los ámbitos de la normalización de las TIC y la certificación de ciberseguridad de las TIC. En particular, en relación con la normalización, facilitaría el establecimiento y la adopción de normas de ciberseguridad. ENISA también ejecutaría las tareas previstas en el contexto del futuro marco de certificación (véase la sección siguiente).
- **Investigación e innovación:** ENISA aportaría sus conocimientos técnicos asesorando a las autoridades nacionales y de la UE sobre la fijación de prioridades de investigación y desarrollo, especialmente en el contexto de la asociación público-privada contractual (APPC) sobre ciberseguridad. Las recomendaciones de ENISA en materia de investigación se trasladarían al nuevo Centro Europeo de Investigación y Competencias sobre Ciberseguridad en virtud del próximo marco financiero plurianual. ENISA también participaría, previa solicitud de la Comisión, en la ejecución de los programas de financiación de la investigación y la innovación de la UE.
- **Cooperación operativa y gestión de crisis:** Esta línea de trabajo debería reforzar las capacidades operativas preventivas existentes, especialmente potenciando los ejercicios paneuropeos en la materia (Cyber Europe) para que se celebren anualmente, y facilitar la cooperación operativa en tanto que secretaría de la red de CSIRT (con arreglo a la Directiva SRI), garantizando, entre otras cosas, el buen funcionamiento de la infraestructura de TI y de los canales de comunicación de la mencionada red. En este contexto, resultaría necesaria una cooperación estructurada con el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) y otros organismos pertinentes de la UE. Además, una cooperación estructurada con el CERT-UE, en estrecha proximidad física, debería desembocar en una función que facilitase asistencia técnica en caso de incidentes significativos y apoyase el análisis de incidentes. Los Estados miembros de la UE que la solicitasen recibirían asistencia para gestionar

incidentes y apoyo para el análisis de vulnerabilidades, artefactos e incidentes a fin de reforzar su propia capacidad de prevención y respuesta.

- ENISA también intervendría en el **plan director de ciberseguridad de la UE** presentado en el marco de este conjunto de medidas y que contiene la recomendación de la Comisión a los Estados miembros para dar una respuesta coordinada a los incidentes y crisis de ciberseguridad de gran escala y carácter transfronterizo a nivel de la UE¹³. ENISA facilitaría la cooperación entre Estados miembros concretos en la gestión de la respuesta de emergencia mediante el análisis y la agregación de los informes de situación nacionales sobre la base de la información que los Estados miembros y otras entidades pongan a disposición de la Agencia de forma voluntaria.

• **Certificación de la ciberseguridad de los productos y servicios de TIC**

A fin de establecer y preservar la confianza y la seguridad, es preciso que los productos y servicios de TIC incorporen directamente las características de seguridad en las etapas iniciales de su diseño y desarrollo técnicos (seguridad a través del diseño). Por otra parte, los clientes y usuarios necesitan poder comprobar el nivel de garantía de la seguridad de los productos y servicios que compran o adquieren.

La certificación, que consiste en la evaluación formal de los productos, servicios y procesos por un organismo independiente y acreditado en función de un conjunto de criterios claramente definidos y la expedición de un certificado que atestigüe la conformidad, desempeña un papel importante a la hora de aumentar la confianza y la seguridad en los productos y servicios. Mientras que la evaluación de la seguridad tiene un carácter bastante técnico, la certificación cumple el objetivo de informar y tranquilizar a los compradores y usuarios sobre las propiedades de seguridad de los productos y servicios de TIC que compran o utilizan. Como ya se ha dicho, esto reviste especial importancia en el caso de los nuevos sistemas que hacen amplio uso de las tecnologías digitales y que requieren un alto nivel de seguridad, como los automóviles conectados y automatizados, la sanidad electrónica, los sistemas de control de la automatización industrial (IACS)¹⁴ o las redes inteligentes.

En la actualidad, el paisaje de la certificación de la ciberseguridad de los productos y servicios de TIC en la UE es muy desigual. Existen diversas iniciativas internacionales, como los denominados criterios comunes para la evaluación de la seguridad de la tecnología de la información (ISO 15408), que es una norma internacional para la evaluación de la seguridad informática. Se basa en la evaluación por un tercero y contempla siete niveles de garantía de la evaluación. Los criterios comunes y la metodología común para la evaluación de la seguridad de la tecnología de la información (CEM) asociada constituyen la base técnica de un acuerdo internacional, el Acuerdo de reconocimiento de los criterios comunes (CCRA), que garantiza que los certificados de criterios comunes sean reconocidos por todos sus signatarios. No obstante, en la versión actual del CCRA solo gozan de reconocimiento mutuo

¹³ El «plan director» se aplicará a los incidentes de ciberseguridad que causen perturbaciones mayores de las que un Estado miembro puede abordar por sí solo o que afecten a dos o más Estados miembros con un impacto de tanta importancia y alcance o tanta significación política que exige una oportuna coordinación de medidas y una respuesta a nivel político de la Unión.

¹⁴ La DG JRC ha publicado un informe que propone un conjunto inicial de requisitos comunes europeos y directrices generales relativos a la certificación de la ciberseguridad de los componentes de IACS. Disponible en: <https://emcip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf>

las evaluaciones hasta el nivel 2. Además, solo trece Estados miembros han firmado el Acuerdo.

Las autoridades de certificación de doce Estados miembros han celebrado un acuerdo de reconocimiento mutuo relativo a los certificados expedidos de conformidad con el Acuerdo sobre la base de los criterios comunes¹⁵. Por otra parte, existen actualmente o se están estableciendo en los Estados miembros una serie de iniciativas de certificación de las TIC. Estas iniciativas, aunque sean importantes, conllevan el riesgo de fragmentar el mercado y provocar problemas de interoperabilidad. En consecuencia, una empresa puede tener que someterse a varios procedimientos de certificación en distintos Estados miembros para poder ofrecer su producto en múltiples mercados. Así, un fabricante de contadores inteligentes que desee vender sus productos en tres Estados miembros, por ejemplo Alemania, Francia y el Reino Unido, tiene que ajustarse actualmente a tres regímenes de certificación diferentes. Se trata del *Commercial Product Assurance* (CPA) en el Reino Unido, la *Certification de Sécurité de Premier Niveau* (CSPN) en Francia y un perfil de protección específico basado en los criterios comunes en Alemania.

Esta situación propicia un incremento de los costes y constituye una carga administrativa considerable para las empresas que operan en varios Estados miembros. Aun cuando el coste de la certificación puede variar considerablemente dependiendo del producto o servicio de que se trate, el nivel de garantía de la evaluación requerido y/u otros componentes, en términos generales suele resultar bastante elevado para las empresas. El certificado *Smart Meter Gateway* del BSI, por ejemplo, tiene un coste superior al millón de euros (nivel más elevado de ensayo y garantía, afecta no solo a un producto, sino a toda la infraestructura que lo rodea). El coste de la certificación de contadores inteligentes en el Reino Unido asciende a casi 150 000 EUR. En Francia, el coste es similar al del Reino Unido, unos 150 000 EUR o más.

Las principales partes interesadas tanto públicas como privadas reconocieron que, en ausencia de un régimen de certificación de la ciberseguridad a escala de la UE, en muchos casos las empresas han de certificarse individualmente en cada Estado miembro, lo que conduce a la fragmentación del mercado. Lo que es más importante, en ausencia de legislación de armonización de la UE para los productos y servicios de TIC, las diferencias en las normas y prácticas de certificación de la ciberseguridad en los Estados miembros pueden crear en la práctica 28 mercados de la seguridad diferentes en la UE, cada uno de ellos con sus propios requisitos técnicos, métodos de ensayo y procedimientos de certificación de la ciberseguridad. Estos enfoques divergentes a nivel nacional pueden provocar, si no se toman medidas adecuadas a nivel de la UE, un importante retraso en la consecución del mercado único digital, ralentizando o anulando los efectos positivos asociados en términos de crecimiento y empleo.

Sobre la base de lo anterior, en el Reglamento propuesto se establece un marco europeo de certificación de la ciberseguridad (el «**Marco**») para los productos y servicios de TIC y se especifican las funciones y tareas esenciales de ENISA en el ámbito de la certificación de la ciberseguridad. La presente propuesta establece un marco general de normas que regulan los regímenes europeos de certificación de la ciberseguridad. La propuesta no introduce

¹⁵ El Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS) incluye a doce Estados miembros más Noruega y ha desarrollado varios perfiles de protección para un número limitado de productos, como la firma digital, el tacógrafo digital y las tarjetas inteligentes. Los participantes trabajan conjuntamente para coordinar la normalización de los perfiles de protección de los criterios comunes, así como el desarrollo de perfiles de protección. Los Estados miembros suelen exigir la certificación SOG-IS en las licitaciones públicas nacionales.

directamente regímenes de certificación operativos, sino que crea un sistema (marco) para el establecimiento de regímenes específicos para productos/servicios de TIC concretos (en lo sucesivo, «regímenes europeos de certificación de la ciberseguridad»). La creación de regímenes europeos de certificación de la ciberseguridad de conformidad con el Marco permitirá que los certificados expedidos con arreglo a dichos regímenes obtengan validez y reconocimiento en todos los Estados miembros y se combata la fragmentación actual del mercado.

El objetivo general de un régimen europeo de certificación de la ciberseguridad es dejar constancia de que los productos y servicios de TIC certificados con arreglo a dicho régimen cumplen unos requisitos de ciberseguridad especificados. Entre ellos figurarían, por ejemplo, su capacidad para proteger los datos (conservados, transmitidos o procesados de la manera que sea) del almacenamiento, tratamiento, acceso, divulgación, destrucción, pérdida o alteración accidentales o no autorizados. Los regímenes de certificación de la ciberseguridad de la UE harían uso de normas existentes en relación con los requisitos técnicos y procedimientos de evaluación que los productos deben cumplir, pero no desarrollarían las normas técnicas en sí¹⁶. Por ejemplo, una certificación a escala de la UE de productos tales como las tarjetas inteligentes, que actualmente se someten a ensayo en función de normas internacionales de criterios comunes en el marco del sistema multilateral (descrito anteriormente) SOG-IS, significaría que el régimen tendría validez en toda la UE.

Además de indicar un conjunto específico de objetivos de seguridad que deben tenerse en cuenta al diseñar un régimen concreto de certificación de la ciberseguridad de la UE, la propuesta establece el contenido mínimo de este tipo de regímenes. Los regímenes tendrán que definir, entre otras cosas, una serie de elementos específicos que determinan el alcance y objeto de la certificación de ciberseguridad. Esto incluye la indicación de las categorías de productos y servicios cubiertos, la especificación detallada de los requisitos de ciberseguridad (por ejemplo, remitiéndose a las normas o especificaciones técnicas pertinentes), los métodos y criterios específicos de evaluación y el nivel de garantía que se proponen asegurar (a saber, básico, sustancial o elevado).

Los regímenes europeos de certificación de la ciberseguridad serán preparados por ENISA con la asistencia, asesoramiento y estrecha cooperación del Grupo Europeo de Certificación de la Ciberseguridad (véase más adelante), y adoptados por la Comisión mediante actos de ejecución. Cuando se detecte la necesidad de un régimen de certificación de la ciberseguridad, la Comisión solicitará a ENISA que prepare un régimen para determinados productos o servicios de TIC. ENISA trabajará al respecto en estrecha colaboración con las autoridades nacionales de supervisión de la certificación representadas en el Grupo. Los Estados miembros y el Grupo podrán proponer a la Comisión que solicite a ENISA la preparación de un régimen particular.

La certificación puede resultar un proceso muy costoso, que podría traducirse en un alza de los precios para los clientes y los consumidores. La necesidad de certificar puede variar también considerablemente en función del contexto específico de uso de los productos y servicios y de la rapidez del cambio tecnológico. El recurso a la certificación europea de la ciberseguridad debe, por tanto, seguir siendo voluntario, a menos que se disponga otra cosa en la legislación de la Unión que establezca los requisitos de seguridad de productos y servicios de TIC.

¹⁶ En el caso de las normas europeas, esto lo efectúan las organizaciones europeas de normalización y lo refrenda la Comisión Europea con la publicación en el *Diario Oficial* (véase el Reglamento 1025/2012).

Con el fin de garantizar la armonización y evitar la fragmentación, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad dejarán de aplicarse a partir de la fecha establecida en el acto de ejecución por el que se adopte este régimen. Además, los Estados miembros deberían abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad existente.

Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o los proveedores de servicios de TIC tendrán la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deberían ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación revocarán la acreditación de un organismo de evaluación de la conformidad cuando no se cumplan, o hayan dejado de cumplirse, las condiciones de la acreditación, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

Con arreglo a la propuesta, las tareas de seguimiento, supervisión y ejecución recaen en los Estados miembros. Los Estados miembros deberán contar con una autoridad de supervisión de la certificación. Esta autoridad estará encargada de supervisar que los organismos de evaluación de la conformidad, así como los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, se ajustan a los requisitos del presente Reglamento y de los pertinentes regímenes europeos de certificación de la ciberseguridad. Las autoridades nacionales de supervisión de la certificación serán competentes para tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio. En la medida que proceda, investigarán el objeto de la reclamación e informarán en un plazo razonable al reclamante sobre el curso y el resultado de la investigación. Además, cooperarán con otras autoridades de supervisión de la certificación y autoridades públicas, por ejemplo mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o a determinados regímenes europeos de certificación de la ciberseguridad.

Por último, la propuesta establece el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»), constituido por las autoridades nacionales de supervisión de la certificación de todos los Estados miembros. La principal tarea del Grupo es asesorar a la Comisión sobre las cuestiones relativas a la política de certificación de la ciberseguridad y trabajar con ENISA en la elaboración de proyectos de regímenes europeos de certificación de la ciberseguridad. ENISA asistirá a la Comisión a encargarse de la secretaría del Grupo y conservará un inventario público actualizado de los regímenes aprobados en virtud del marco europeo de certificación de la ciberseguridad. ENISA también mantendrá contactos con los organismos de normalización a fin de garantizar la adecuación de las normas utilizadas en regímenes autorizados y detectar ámbitos que precisen de normas de ciberseguridad.

El marco europeo de certificación de la ciberseguridad (en lo sucesivo, «el Marco») aportará diversos beneficios a los ciudadanos y las empresas. En particular:

- La creación de sistemas de certificación de la ciberseguridad a escala de la UE para determinados productos o servicios proporcionará a las empresas una «ventanilla única» para la certificación de la ciberseguridad en la UE. Las empresas estarán en

condiciones de certificar su producto una sola vez y obtener un certificado válido en todos los Estados miembros. No estarán obligadas a volver a certificar sus productos ante diferentes organismos nacionales de certificación. De este modo disminuirán significativamente los costes para las empresas, se facilitarán las operaciones transfronterizas y, en última instancia, se reducirá y evitará la fragmentación del mercado interior de los productos de que se trate.

- El Marco establece la primacía de los regímenes europeos de certificación de la ciberseguridad sobre los nacionales. Por ello, la adopción de un régimen europeo de certificación de la ciberseguridad sustituirá a todos los regímenes nacionales paralelos existentes para los mismos productos o servicios de TIC a un determinado nivel de garantía. Esto aportará más claridad, reduciendo la actual proliferación de regímenes nacionales de certificación de la ciberseguridad que se solapan y posiblemente se contradicen.
- La propuesta sostiene y complementa la aplicación de la Directiva SRI, proporcionando a las empresas sometidas a ella una herramienta muy útil para demostrar el cumplimiento de los requisitos de la SRI en el conjunto de la Unión. Al desarrollar nuevos regímenes de certificación de la ciberseguridad, la Comisión y ENISA prestarán especial atención a la necesidad de garantizar que los requisitos de SRI se vean reflejados en dichos regímenes.
- La propuesta respaldará y facilitará el desarrollo de una política europea de ciberseguridad, armonizando las condiciones y los requisitos sustantivos para la certificación de la ciberseguridad de los productos y servicios de TIC en la UE. Los regímenes europeos de certificación de la ciberseguridad harán referencia a normas o criterios comunes de evaluación y metodologías de ensayo. De este modo, se contribuirá de manera significativa, aunque indirecta, a la asimilación de soluciones de seguridad comunes en la UE y, por ende, a la eliminación de obstáculos al mercado interior.
- El Marco está concebido con vistas a garantizar la flexibilidad necesaria para los regímenes de certificación de la ciberseguridad. En función de las necesidades específicas en materia de ciberseguridad, un producto o servicio podrá ser certificado en función de niveles de seguridad más o menos elevados. Los regímenes europeos de certificación de la ciberseguridad se diseñarán teniendo en mente esta flexibilidad y, por lo tanto, aportarán distintos niveles de garantía (a saber, básico, sustancial o elevado) con el fin de que puedan usarse con fines distintos o en contextos diferentes.
- En virtud de todos los elementos mencionados, la certificación de la ciberseguridad resultará más atractiva para las empresas como medio eficaz de comunicar el nivel de garantía de la ciberseguridad de los productos o servicios de TIC. En la medida en que la certificación de la ciberseguridad resulte más barata, eficaz y comercialmente atractiva, las empresas tendrán un mayor incentivo para certificar sus productos frente a los riesgos en materia de ciberseguridad, contribuyendo así a la difusión de las mejores prácticas de ciberseguridad en el diseño de productos y servicios de TIC (ciberseguridad a través del diseño).

- **Coherencia con las disposiciones existentes en la misma política sectorial**

En virtud de la Directiva SRI, los operadores de los sectores que son vitales para nuestra economía y sociedad, como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad y la infraestructura digital, así como los proveedores de

servicios digitales (por ejemplo, motores de búsqueda, servicios de computación en la nube y mercados en línea) están obligados a tomar las medidas necesarias para gestionar adecuadamente los riesgos para la seguridad. Las nuevas normas de la presente propuesta complementan las disposiciones de la Directiva SRI y garantizan la coherencia con ellas para fortalecer la ciberresiliencia de la UE mediante la mejora de las capacidades, la cooperación, la gestión de riesgos y la sensibilización.

Por otra parte, las normas sobre certificación de la ciberseguridad ponen una herramienta esencial en manos de las empresas sujetas a la Directiva SRI, dado que podrán certificar sus productos y servicios de TIC frente a los riesgos de ciberseguridad sobre la base de regímenes de certificación de la ciberseguridad válidos y reconocidos en todo el territorio de la UE. También serán complementarias de los requisitos de seguridad mencionados en el Reglamento eIDAS¹⁷ y la Directiva sobre equipos radioeléctricos¹⁸.

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

El Reglamento (UE) 2016/679 (Reglamento general de protección de datos o «**RGPD**»)¹⁹ contiene disposiciones para establecer mecanismos de certificación y sellos y marcas de protección de datos a fin de demostrar la conformidad con el Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del RGPD, incluso cuando dichas operaciones se encuentran integradas en productos y servicios.

El Reglamento propuesto garantizará la compatibilidad con el Reglamento (CE) n.º 765/2008 sobre los requisitos de acreditación y de vigilancia del mercado²⁰ haciendo referencia a las normas de dicho marco sobre los organismos nacionales de acreditación y de evaluación de la conformidad. En lo que respecta a las autoridades de supervisión, el Reglamento propuesto exigirá que los Estados miembros designen autoridades nacionales de supervisión de la certificación responsables de la supervisión, el seguimiento y la ejecución de las normas. Estos organismos serán independientes de los organismos de evaluación de la conformidad prescritos en el Reglamento (CE) n.º 765/2008.

¹⁷ Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

¹⁸ Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE.

¹⁹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

²⁰ Reglamento (CE) n.º 765/2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica de la acción de la UE es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que se refiere a la aproximación de las legislaciones de los Estados miembros a fin de alcanzar los objetivos del artículo 26 del TFUE, a saber, el correcto funcionamiento del mercado interior.

La base jurídica relativa al mercado interior para la creación de ENISA fue respaldada por el Tribunal de Justicia (asunto C-217/04 *Reino Unido contra Parlamento Europeo y Consejo*) y confirmada nuevamente por el Reglamento de 2013 que estableció el mandato actual de la Agencia. Además, las actividades que reflejasen los objetivos de aumentar la cooperación y la coordinación entre los Estados miembros y añadiesen capacidades a nivel de la UE para complementar la acción de los Estados miembros entrarían en la categoría de «cooperación operativa». La Directiva SRI (cuya base jurídica es el artículo 114 del TFUE) la señala específicamente como objetivo que debe perseguirse en el marco de la red de CSIRT, pues «ENISA se hará cargo de la secretaría y apoyará activamente la cooperación» (artículo 12, apartado 2). En particular, el artículo 12, apartado 3, letra f), indica también la identificación de otras formas de cooperación operativa como tarea de la red de CSIRT, en particular en relación con: i) categorías de riesgos e incidentes, ii) alertas tempranas, iii) asistencia mutua, y iv) principios y modalidades de coordinación, cuando los Estados miembros respondan a incidentes y riesgos transfronterizos.

- La actual fragmentación de los regímenes de certificación de productos y servicios de TIC es también consecuencia de la falta de un marco común, eficaz y jurídicamente vinculante, aplicable a los Estados miembros. Esto dificulta la creación de un mercado interior de productos y servicios de TIC y obstaculiza la competitividad de la industria europea en el sector. La presente propuesta tiene por objeto combatir la fragmentación existente y los obstáculos relacionados con el mercado interior ofreciendo un marco común para el establecimiento de regímenes de certificación de la ciberseguridad válidos en toda la UE.

Subsidiariedad (en el caso de competencia no exclusiva)

El principio de subsidiariedad exige evaluar la necesidad y el valor añadido de la acción de la UE. El respeto de la subsidiariedad en este ámbito se reconoció ya en el momento de adoptar el actual Reglamento de ENISA²¹.

La ciberseguridad es una cuestión de interés común de la Unión. Las interdependencias entre las redes y los sistemas de información son tales que muy a menudo los diferentes agentes (públicos y privados, incluidos los ciudadanos) no pueden hacer frente por sí solos a las amenazas y gestionar los riesgos y las posibles repercusiones de los ciberincidentes. Por una parte, las interdependencias entre los Estados miembros, en particular en lo que se refiere a la explotación de las infraestructuras críticas (energía, transporte o agua, por citar solo algunas) hacen que la intervención pública a nivel europeo resulte no solo beneficiosa, sino también necesaria. Por otra, la intervención de la UE puede aportar un efecto «de contagio» positivo

²¹ Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004.

gracias al intercambio de buenas prácticas entre los Estados miembros, lo que puede dar lugar a una mejora de la ciberseguridad de la Unión.

En resumen, en el contexto actual y teniendo en cuenta las perspectivas de futuro, parece que si se quiere **incrementar la ciberresiliencia colectiva** de la Unión, las **actuaciones individuales de sus Estados miembros y un enfoque fragmentado en materia de ciberseguridad** no serán suficientes.

La intervención de la UE también se considera necesaria para hacer frente a la fragmentación de los actuales regímenes de certificación de la ciberseguridad. Permitiría que los fabricantes se beneficiasen plenamente de un mercado interior, con ahorros significativos en relación con los costes de ensayo y rediseño. Aun cuando el actual Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS) ha logrado, por ejemplo, resultados considerables en este sentido, también ha acusado limitaciones importantes que merman su idoneidad para ofrecer soluciones sostenibles a largo plazo que permitan aprovechar todas las posibilidades del mercado interior.

El valor añadido de la actuación a nivel de la UE, en particular para reforzar la cooperación entre los Estados miembros, pero también entre las comunidades de la seguridad de las redes y de la información, fue reconocido por las Conclusiones del Consejo de 2016²² y también se desprende claramente de la evaluación de ENISA.

- **Proporcionalidad**

La medida propuesta no excede de lo necesario para alcanzar sus objetivos. Además, el ámbito de la intervención de la UE no impide ulteriores medidas nacionales en el campo de la seguridad nacional. Por lo tanto, la acción de la UE está justificada en cuanto a la subsidiariedad y la proporcionalidad.

- **Elección del instrumento**

La presente propuesta revisa el Reglamento (UE) n.º 526/2013, que establece el mandato y las tareas actuales de ENISA. Además, habida cuenta del importante papel de ENISA en la creación y gestión de un marco de certificación de la ciberseguridad de la UE, conviene establecer el nuevo mandato de ENISA y el citado marco en un único instrumento jurídico, utilizando como instrumento un Reglamento.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

Evaluaciones *ex post* / control de calidad de la legislación existente

La Comisión, de acuerdo con la hoja de ruta de la evaluación²³, evaluó la **pertinencia, repercusión, eficacia, eficiencia, coherencia y valor añadido** de la Agencia en lo que se refiere a su rendimiento, gobernanza, estructura organizativa interna y prácticas de trabajo durante el período 2013-2016. Los resultados principales pueden resumirse del siguiente

²² Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

²³ http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

modo (para más información, véase el documento de trabajo de los servicios sobre el tema, que acompaña a la evaluación de impacto).

- **Pertinencia:** En un contexto de avances tecnológicos y amenazas cambiantes, y teniendo en cuenta la significativa necesidad de reforzar la ciberseguridad en la UE, los objetivos de ENISA se han demostrado pertinentes. De hecho, los Estados miembros y los organismos de la UE confían en sus sustanciales conocimientos en materia de ciberseguridad. Además, deben desarrollarse en los Estados miembros capacidades que permitan comprender y responder mejor a las amenazas, y es precisa una cooperación de las partes interesadas de todos los ámbitos temáticos e instituciones. La ciberseguridad sigue siendo una prioridad política clave de la UE a la que se espera responda ENISA; sin embargo, el diseño de ENISA como agencia de la UE con un mandato de duración determinada: i) no permite una planificación a largo plazo y un apoyo sostenible a los Estados miembros y las instituciones de la UE, ii) puede dar lugar a un vacío legal en la medida en que las disposiciones de la Directiva SRI encomiendan a ENISA tareas de carácter permanente²⁴, iii) carece de coherencia con una visión que vincule a ENISA con un ecosistema de ciberseguridad de la UE reforzado.
- **Eficacia:** ENISA alcanzó en general sus objetivos y desempeñó sus cometidos. Contribuyó al incremento de la seguridad de las redes y de la información en Europa por medio de sus actividades principales (creación de capacidades, asistencia técnica, creación de comunidades y apoyo a las políticas). Sin embargo, mostró que había margen de mejora en relación con cada una de ellas. La evaluación llegó a la conclusión de que ENISA ha creado efectivamente unas relaciones sólidas y de confianza con algunas de sus partes interesadas, especialmente con los Estados miembros y la comunidad de CSIRT. Las intervenciones en materia de creación de capacidades se consideraron eficaces, en particular en los Estados miembros que cuentan con menos recursos. El estímulo de una amplia cooperación ha sido uno de los aspectos más destacados, coincidiendo las partes interesadas en el papel positivo que desempeña ENISA para acercar a las personas. Sin embargo, ENISA encontró dificultades para lograr un impacto notable en el extenso campo de la seguridad de las redes y de la información. Ello se debió también al hecho de que dispuso de unos recursos humanos y financieros bastante limitados para cumplir un mandato muy amplio. La evaluación también llegó a la conclusión de que ENISA alcanzó parcialmente el objetivo de proporcionar asesoramiento, dados los problemas para contratar expertos (véase también la sección sobre eficiencia).
- **Eficiencia:** A pesar de su reducido presupuesto (entre los más bajos de las agencias de la UE), la Agencia ha sido capaz de contribuir a alcanzar objetivos concretos, demostrando una eficiencia global en el uso de sus recursos. La evaluación concluyó que los procesos eran por regla general eficientes y que la clara delimitación de responsabilidades dentro de la organización propiciaba una buena ejecución del trabajo. Uno de los principales retos para la eficiencia de la Agencia guarda relación con las dificultades de ENISA para contratar y retener a expertos altamente cualificados. Las conclusiones muestran que esto se puede explicar por una combinación de factores, entre los que figuran las dificultades de carácter general del sector público para competir con el privado en la contratación de expertos altamente

²⁴

Referencia a los artículos 7, 9, 11, 12 y 19 de la Directiva sobre Seguridad de las Redes y los Sistemas de Información (Directiva SRI).

especializados, el tipo de contrato (temporal) que la Agencia podría ofrecer básicamente y el escaso atractivo de la ubicación de ENISA en lo que se refiere, por ejemplo, a las dificultades de los cónyuges para encontrar trabajo. La doble localización en Atenas y Heraklion exigió esfuerzos adicionales de coordinación y generó costes suplementarios, pero el traslado a Atenas en 2013 del departamento de operaciones esenciales reforzó la eficacia operativa de la Agencia.

- **Coherencia:** Las actividades de ENISA han sido coherentes por regla general con las políticas y actividades de las partes interesadas, a escala nacional y de la UE, pero es necesario un enfoque más coordinado a nivel de la UE en materia de ciberseguridad. No se ha aprovechado plenamente el potencial para la cooperación entre ENISA y otros organismos de la UE. La evolución del panorama jurídico y político de la UE hace que el vigente mandato resulte menos coherente en la actualidad.
- **Valor añadido de la UE:** El valor añadido de ENISA radica principalmente en la capacidad de la Agencia para mejorar la cooperación, principalmente entre los Estados miembros, pero también con las comunidades de la seguridad de las redes y de la información relacionadas. No existe ningún otro agente a nivel de la UE que facilite la cooperación de una variedad análoga de partes interesadas en la seguridad de las redes y de la información. El valor añadido aportado por la Agencia osciló en función de las diferentes necesidades y recursos de sus partes interesadas (por ejemplo, Estados miembros grandes o pequeños; Estados miembros e industria) y de la necesidad de que la Agencia priorizase sus actividades con arreglo al programa de trabajo. La evaluación llegó a la conclusión de que una eventual clausura de ENISA representaría la pérdida de una oportunidad para todos los Estados miembros. No será posible garantizar el mismo grado de creación de comunidades y cooperación en los Estados miembros en el ámbito de la ciberseguridad. Sin una agencia de la UE más centralizada, la fragmentación aumentaría y la cooperación bilateral o regional intentaría colmar el vacío dejado por ENISA.

En lo que se refiere concretamente al rendimiento pasado y al futuro de ENISA, las principales tendencias que se desprenden de la consulta de 2017 son las siguientes²⁵:

- El rendimiento global de ENISA durante el período de 2013 a 2016 fue evaluado positivamente en la mayoría de las respuestas (74 %). También fue mayoritaria la opinión de que ENISA estaba alcanzando sus diferentes objetivos (al menos un 63 % para cada uno de los objetivos). Los servicios y productos de ENISA son utilizados de forma regular (mensualmente o con mayor frecuencia) por casi la mitad de quienes respondieron (46 %) y apreciados por el hecho de proceder de un organismo a nivel de la UE (83 %) y por su calidad (62 %).
- En las respuestas se mencionan diversas lagunas y retos para el futuro de la ciberseguridad en la UE, siendo los cinco principales (en una lista de 16): la

²⁵

Respondieron a la consulta 90 partes interesadas procedentes de 19 Estados miembros (88 respuestas y 2 documentos de posición), incluidas las autoridades nacionales de 15 Estados miembros, incluidos Francia, Italia, Irlanda y Grecia y 8 organizaciones representativas de un gran número de organizaciones europeas, como por ejemplo la Federación Bancaria Europea, Europa Digital (en representación de la industria de la tecnología digital en Europa) o la Asociación de Operadores Europeos de Redes de Telecomunicación (ETNO). La consulta pública sobre ENISA se complementó con otras fuentes diversas, entre ellas: i) entrevistas en profundidad con unos 50 agentes clave del colectivo de la ciberseguridad, ii) una encuesta a la red de CSIRT, iii) una encuesta al Consejo de Administración, al Comité Ejecutivo y al Grupo Permanente de Partes Interesadas de ENISA.

cooperación entre los Estados miembros; la capacidad para prevenir, detectar y solucionar los ciberataques a gran escala; la cooperación entre los Estados miembros en las cuestiones relacionadas con la ciberseguridad; la cooperación y el intercambio de información entre las distintas partes interesadas, incluida la cooperación entre los sectores público y privado; la protección de las infraestructuras críticas frente a ciberataques.

- Una gran mayoría (88 %) de las respuestas consideraba que los actuales instrumentos y mecanismos disponibles a nivel de la UE son insuficientes o adecuados solo parcialmente para abordar estos problemas. Una gran mayoría de las respuestas (98 %) indicó que un organismo de la UE debía dar respuesta a estas necesidades y, entre ellos, el 99 % consideraba que ENISA era la organización adecuada para ello.

Consultas con las partes interesadas

- La Comisión organizó una consulta pública para la revisión de ENISA, abierta entre el 12 de abril y el 5 de julio de 2016, y recibió 421 respuestas²⁶. Según los resultados, el 67,5 % de las respuestas expresaron la opinión de que ENISA podría desempeñar cierto papel en el establecimiento de un marco armonizado para la certificación de la seguridad de los productos y servicios de TI.

Los resultados de la consulta de 2016 sobre la APP contractual de ciberseguridad²⁷, en la sección relativa a la certificación, muestran que:

- El 50,4 % (121 de 240) desconoce si los regímenes nacionales de certificación están reconocidos mutuamente en los Estados miembros de la UE. El 25,8 % (62 de 240) responde «no», mientras que el 23,8 % (57 de 240) responde «sí».
- El 37,9 % de las respuestas (91 de 240) considera que los actuales regímenes de certificación no atienden las necesidades de la industria europea. Por otra parte, en 17,5 % (42 de 240), principalmente empresas internacionales que operan en el mercado europeo, opina lo contrario.
- El 49,6 % (119 de 240) de las respuestas afirma que no es fácil demostrar la equivalencia entre normas, regímenes de certificación y etiquetas. El 37,9 % (91 de 240) responde «no lo sé», mientras que solo el 12,5 % (30 de 240) responde «sí».

Obtención y uso de asesoramiento especializado

La Comisión se basó en el siguiente asesoramiento externo:

- *Study on the Evaluation of ENISA* (Estudio de evaluación de ENISA) (Ramboll/Carsa 2017; SMART n.º 2016/0077),
- *Study on ICT Security Certification and labelling – Evidence gathering and impact assessment* (Estudio sobre certificación y el etiquetado de seguridad de las TIC —

²⁶ A saber, 162 contribuciones de ciudadanos, 33 de organizaciones de consumidores y de la sociedad civil, 186 del sector y 40 de las administraciones públicas, incluidas las autoridades competentes encargadas de la aplicación de la Directiva sobre privacidad y comunicaciones electrónicas.

²⁷ Respondieron a la sección relativa a la certificación 240 representantes de las administraciones públicas nacionales, las grandes empresas, las pymes, las microempresas y los organismos de investigación.

Evaluación de impacto

El informe de evaluación de impacto sobre esta iniciativa señaló los siguientes problemas principales que deben abordarse:

- fragmentación de las políticas y enfoques en materia de ciberseguridad en los distintos Estados miembros;
- dispersión de los recursos y fragmentación de los enfoques en materia de ciberseguridad en las instituciones, órganos y organismos de la UE; e
- insuficiencia de los conocimientos e información de los ciudadanos y las empresas, junto con la creciente aparición de múltiples regímenes de certificación nacionales y sectoriales.

El informe evaluó las siguientes posibles opciones en relación con el mandato de ENISA:

- mantenimiento del *statu quo*, es decir, mandato ampliado pero todavía limitado en el tiempo (opción de referencia);
- expiración del mandato actual de ENISA sin renovación y cierre de ENISA (ausencia de intervención);
- una «reforma de ENISA»; y
- una agencia de ciberseguridad de la UE con plena capacidad operativa.

El informe evaluó las siguientes posibles opciones en relación con la certificación de la ciberseguridad:

- ausencia de intervención (opción de referencia);
- medidas no legislativas (Derecho indicativo);
- un acto legislativo de la Unión con el fin de crear un régimen obligatorio para todos los Estados miembros basado en el sistema SOG-IS; y
- un marco general de certificación de la ciberseguridad de las TIC en la UE.

El análisis llevó a la conclusión de que la opción preferida es una «reforma de ENISA», combinada con un marco general de la UE para la certificación de la ciberseguridad de las TIC.

La opción preferida ha sido considerada la más eficaz para que la UE alcance los objetivos de: aumentar las capacidades de ciberseguridad, preparación, cooperación, sensibilización, transparencia y evitación de la fragmentación del mercado. También la más coherente con las prioridades políticas de la Estrategia de Ciberseguridad de la UE y sus demás políticas relacionadas (por ejemplo, la Directiva SRI) y la Estrategia para el Mercado Único Digital. Además, el proceso de consulta puso de manifiesto que la opción preferida cuenta con el apoyo de la mayoría de las partes interesadas. El análisis efectuado en la evaluación de impacto mostró asimismo que la opción preferida permitiría alcanzar los objetivos mediante un empleo razonable de los recursos.

El Comité de Control Reglamentario de la Comisión emitió inicialmente un dictamen negativo el 24 de julio, y posteriormente un dictamen favorable tras una nueva presentación el 25 de agosto de 2017. El informe de evaluación de impacto modificado incorporaba nuevos

justificativos, las conclusiones finales de la evaluación de ENISA y explicaciones adicionales sobre las opciones políticas y su impacto. El anexo 1 del informe final sobre la evaluación de impacto resume cómo se había respondido a las observaciones del Comité en el segundo dictamen. En particular, se actualizó el informe para incorporar con mayor detalle el contexto de ciberseguridad de la UE, incluidas las medidas que figuran en la Comunicación conjunta «Resiliencia, disuasión y defensa: Reforzar la ciberseguridad de la UE» [JOIN(2017) 450] y tienen una especial relevancia para ENISA: el plan director de ciberseguridad de la UE y el Centro Europeo de Investigación y Competencias sobre Ciberseguridad, al que la Agencia sometería sus recomendaciones sobre las necesidades de la UE en materia de investigación.

El informe explica cómo la reforma de la Agencia, incluidas las nuevas funciones, las mejores condiciones de empleo y la cooperación estructural con los órganos de la UE en este ámbito, podría mejorar su atractivo como empleador y ayudar a afrontar los problemas relacionados con la contratación de expertos. El anexo 6 del informe presenta también una estimación revisada de los costes asociados a las opciones políticas de ENISA. En relación con el tema de la certificación, se ha revisado el informe con el fin de proporcionar una explicación más detallada, incluida una presentación gráfica, de la opción preferida, y de ofrecer estimaciones sobre los costes para los Estados miembros y la Comisión en relación con el nuevo marco de certificación. También se ha justificado la elección de ENISA como agente clave en el marco sobre la base de su experiencia en este ámbito y el hecho de ser la única agencia de ciberseguridad a nivel de la UE. Por último, se han revisado las secciones sobre certificación para aclarar los aspectos relacionados con la diferencia con el actual sistema SOG-IS y los beneficios asociados a las diferentes opciones y para explicar el hecho de que el tipo de producto y servicio de TIC cubierto por un régimen europeo de certificación se defina en el propio régimen aprobado.

Adecuación regulatoria y simplificación

No procede

Impacto en los derechos fundamentales

La ciberseguridad desempeña un papel esencial en la protección de los datos personales y la intimidad de las personas físicas de conformidad con lo dispuesto en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE. Cuando se produce un ciberincidente, la intimidad y la protección de nuestros datos personales quedan claramente en entredicho. La ciberseguridad es, pues, condición necesaria para el respeto de la intimidad y la confidencialidad de nuestros datos personales. Desde esta perspectiva, con el objetivo de reforzar la ciberseguridad en Europa, la propuesta constituye un importante complemento de la legislación vigente que protege el derecho fundamental al respeto de la intimidad y de los datos personales. La ciberseguridad es esencial asimismo para proteger la confidencialidad de nuestras comunicaciones electrónicas y, por tanto, para ejercer la libertad de expresión y de información y otros derechos afines, tales como la libertad de pensamiento, conciencia y religión.

4. REPERCUSIONES PRESUPUESTARIAS

Véase la ficha financiera

5. OTROS ELEMENTOS

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

La Comisión supervisará la aplicación del Reglamento y presentará cada cinco años un informe sobre su evaluación al Parlamento Europeo y al Consejo, así como al Comité Económico y Social Europeo. Estos informes serán públicos y analizarán la aplicación y el cumplimiento efectivos del presente Reglamento.

- **Explicación detallada de las disposiciones específicas de la propuesta**

El título I del Reglamento contiene las disposiciones generales: el objeto (artículo 1), las definiciones (artículo 2), incluidas las referencias a las definiciones pertinentes de otros instrumentos de la UE, como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI), el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93, y el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, sobre la normalización europea.

El título II del Reglamento contiene las disposiciones clave relacionadas con ENISA, la Agencia de Ciberseguridad de la UE.

El capítulo I de este título describe el mandato (artículo 3), los objetivos (artículo 4) y las funciones de la Agencia (artículos 5 a 11).

El capítulo II describe la organización de ENISA y contiene disposiciones fundamentales sobre su estructura (artículo 12). Aborda la composición, las normas de votación y las funciones del Consejo de Administración (sección 1, artículos 13 a 17), del Comité Ejecutivo (sección 2, artículo 18) y del director ejecutivo (Sección 3, artículo 19). También incluye disposiciones sobre la composición y funciones del Grupo Permanente de Partes Interesadas (Sección 4, artículo 20). Por último, la sección 5 del capítulo detalla las normas operativas de la Agencia, en particular en lo que respecta a la programación de sus operaciones, conflictos de intereses, transparencia, confidencialidad y acceso a los documentos (artículos 21 a 25).

El capítulo III se refiere al establecimiento y la estructura del presupuesto de la Agencia (artículos 26 y 27), así como a las normas que rigen su aplicación (artículos 28 y 29). Incluye, asimismo, disposiciones para facilitar la lucha contra el fraude, la corrupción y otras actividades ilícitas (artículo 30).

El capítulo IV se refiere a la dotación de personal de la Agencia. Incluye disposiciones generales sobre el Estatuto y el Régimen aplicable y las normas sobre privilegios e inmunidades (artículo 31 y 32). Asimismo, se detallan las normas de contratación y nombramiento del director ejecutivo de la Agencia (artículo 33). Por último, incluye las disposiciones que rigen la utilización de expertos nacionales en comisión de servicios u otro personal no contratado por la Agencia (artículo 34).

Finalmente, el capítulo V reúne las disposiciones generales relativas a la Agencia. Indica su estatuto jurídico (artículo 35) e incluye disposiciones que regulan las cuestiones de responsabilidad, régimen lingüístico, protección de los datos personales (artículos 36-38), así como las normas de seguridad sobre la protección de la información clasificada y de la información sensible no clasificada (artículo 40). En él se describen las normas que regulan la cooperación de la Agencia con terceros países y organizaciones internacionales (artículo 39). Por último, contiene disposiciones relativas a la sede de la Agencia y las condiciones

operativas, así como al control administrativo por parte del Defensor del Pueblo (artículos 41 y 42).

El título III del Reglamento establece el marco europeo de certificación de la ciberseguridad (el «**Marco**») para los productos y servicios de TIC como *lex generalis* (artículo 1). Define el objetivo general de los regímenes europeos de certificación de la ciberseguridad, a saber, garantizar que los productos y servicios de TIC cumplan los requisitos de ciberseguridad especificados en lo que respecta a su capacidad para resistir, con un nivel de garantía dado, las acciones que comprometan la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados, o las funciones relacionadas o los servicios (artículo 43). Por otra parte, enumera los objetivos de seguridad que deben proponerse los regímenes europeos de certificación de la ciberseguridad (artículo 45), como por ejemplo la capacidad para proteger los datos del acceso o la revelación, destrucción o alteración accidentales o no autorizados y el contenido (es decir, los elementos) de los regímenes europeos de certificación de la ciberseguridad, por ejemplo la definición detallada de su ámbito de aplicación, los objetivos de seguridad, los criterios de evaluación, etc. (artículo 47).

El título III establece también los principales efectos jurídicos de los regímenes europeos de certificación de la ciberseguridad, a saber, i) la obligación de aplicar el régimen a nivel nacional y el carácter voluntario de la certificación, ii) el hecho de que los regímenes europeos de certificación de la ciberseguridad invaliden los regímenes nacionales relativos a los mismos productos o servicios (artículos 48 y 49).

Este título establece asimismo el procedimiento para la adopción de los regímenes europeos de certificación de la ciberseguridad y las funciones respectivas de la Comisión, ENISA y el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») (artículo 44). Por último, establece las disposiciones relativas a los organismos de evaluación de la conformidad, incluidos sus requisitos, competencias y funciones, las autoridades nacionales de supervisión de la certificación y las sanciones.

Se establece asimismo en este título el Grupo como organismo esencial integrado por representantes de las autoridades nacionales de supervisión de la certificación, cuya función principal es trabajar con ENISA en la preparación de los regímenes europeos de certificación de la ciberseguridad y asesorar a la Comisión sobre cuestiones generales o específicas relativas a la política de certificación de la ciberseguridad.

El título IV del Reglamento contiene las disposiciones finales que describen el ejercicio de la delegación, los requisitos de evaluación, la derogación y sucesión, así como la entrada en vigor.

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»)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Prevía transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo²⁸,

Visto el dictamen del Comité de las Regiones²⁹,

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

- (1) Las redes y los sistemas de información y las redes y servicios de telecomunicaciones desempeñan un papel vital para la sociedad y se han convertido en la espina dorsal del crecimiento económico. Las tecnologías de la información y la comunicación están en la base de los complejos sistemas que sustentan las actividades de la sociedad, garantizan el funcionamiento de nuestras economías en sectores clave como la salud, la energía, las finanzas y el transporte y, en particular, respaldan el funcionamiento del mercado interior.
- (2) La utilización de las redes y los sistemas de información por los ciudadanos, empresas y administraciones de toda la Unión está ya muy generalizada. La digitalización y la conectividad se convierten en elementos básicos en un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera el despliegue en la UE de millones, si no miles de millones, de dispositivos digitales conectados durante la próxima década. Mientras aumenta el número de dispositivos conectados a internet, la seguridad y la resiliencia no se tienen suficientemente en cuenta desde el diseño, lo que provoca insuficiencias en la ciberseguridad. En este contexto, el uso limitado de la certificación priva a los usuarios individuales y las organizaciones de información suficiente sobre las características de ciberseguridad de los productos y servicios de TIC y socava la confianza en las soluciones digitales.
- (3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más

²⁸ DO C [...] de [...], p. [...].

²⁹ DO C [...] de [...], p. [...].

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

- (4) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y ciberataques, requieren unas defensas más sólidas. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las respuestas políticas de las autoridades de ciberseguridad y las competencias policiales son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la UE. Esta situación requiere una respuesta y una gestión de crisis efectivas a nivel de la UE, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad europea y la asistencia mutua. En consecuencia, también una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables, y una previsión sistemática de los futuros avances, retos y amenazas, tanto en la Unión como en el mundo, son importantes para los responsables políticos, la industria y los usuarios.
- (5) A la luz de los crecientes retos que tiene planteados la Unión en materia de ciberseguridad, es necesario un conjunto completo de medidas que se apoye en actuaciones previas de la Unión y promueva objetivos que se refuercen mutuamente. Entre ellas se incluye la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación y la coordinación en los Estados miembros y las instituciones, órganos y organismos de la UE. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades a nivel de la Unión que podrían complementar la acción de los Estados miembros, en particular en caso de ciberincidentes y crisis transfronterizas a gran escala. Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones de ciberseguridad. Además, debe reforzarse la confianza en el mercado único digital ofreciendo información transparente sobre el nivel de seguridad de los productos y servicios de TIC. Esto puede verse facilitado por una certificación a escala de la UE que aporte requisitos y criterios de evaluación de la ciberseguridad comunes en todos los mercados y sectores nacionales.
- (6) En 2004 el Parlamento Europeo y el Consejo adoptaron el Reglamento (CE) n.º 460/2004³⁰ por el que se creaba ENISA con el objetivo de contribuir a garantizar un nivel efectivo y elevado de seguridad de las redes y de la información dentro de la Unión y a desarrollar una cultura de la seguridad de las redes y de la información en beneficio de ciudadanos, consumidores, empresas y administraciones públicas. En 2008, el Parlamento Europeo y el Consejo adoptaron el Reglamento (CE) n.º 1007/2008³¹, que prorrogaba el mandato de la Agencia hasta marzo de 2012. El

³⁰ Reglamento (CE) n.º 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

³¹ Reglamento (CE) n.º 1007/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, que modifica el Reglamento (CE) n.º 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, en lo que respecta a su duración (DO L 293 de 31.10.2008, p. 1).

Reglamento (CE) n.º 580/2011³² prorrogó nuevamente dicho mandato hasta el 13 de septiembre de 2013. En 2013, el Parlamento Europeo y el Consejo adoptaron el Reglamento (UE) n.º 526/2013³³ relativo a ENISA y por el que se derogaba el Reglamento (CE) n.º 460/2004, que prorrogaba el mandato de la Agencia hasta junio de 2020.

- (7) La Unión ha adoptado ya medidas importantes para garantizar la ciberseguridad y aumentar la confianza en las tecnologías digitales. En 2013, se adoptó una Estrategia de ciberseguridad de la UE para orientar la respuesta política de la Unión a las amenazas y riesgos relacionados con la ciberseguridad. En su esfuerzo por proteger mejor a los europeos en línea, la Unión adoptó en 2016 el primer acto legislativo en el ámbito de la ciberseguridad, la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en lo sucesivo, «Directiva SRI»). La Directiva SRI instauró requisitos relativos a las capacidades nacionales en el ámbito de la ciberseguridad, estableció los primeros mecanismos para mejorar la cooperación estratégica y operativa entre los Estados miembros e introdujo obligaciones relativas a medidas de seguridad y notificaciones de incidentes en todos los sectores fundamentales para la economía y la sociedad, como la energía, los transportes, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad, las infraestructuras digitales, así como los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea). Se atribuyó un papel clave a ENISA para respaldar la aplicación de esta Directiva. Además, una lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, contribuyendo al objetivo general de conseguir un elevado nivel de ciberseguridad.
- (8) Se reconoce que, desde la adopción de la Estrategia de ciberseguridad de la UE de 2013 y la última revisión del mandato de la Agencia, el contexto político general ha cambiado considerablemente, en particular en relación con un contexto mundial más incierto y menos seguro. En este contexto, y en el marco de la nueva política de ciberseguridad de la Unión, es necesario revisar el mandato de ENISA para definir su función en el ecosistema en mutación de la ciberseguridad y garantizar que contribuya eficazmente a configurar la respuesta de la Unión a los desafíos derivados de esta transformación radical del panorama de las amenazas, para lo cual no basta, como reconoció la evaluación de la Agencia, el actual mandato.
- (9) La Agencia establecida por el presente Reglamento debe suceder a ENISA, tal como fue establecida por el Reglamento (UE) n.º 526/2013. La Agencia debe llevar a cabo las tareas que le confiere el presente Reglamento y los actos jurídicos de la Unión en el ámbito de la ciberseguridad aportando, entre otras cosas, conocimientos y asesoramiento y actuando como centro de información y conocimientos de la Unión. Debe fomentar el intercambio de mejores prácticas entre los Estados miembros y las partes interesadas del sector privado, sugiriendo políticas a la Comisión Europea y los Estados miembros, actuando como punto de referencia para las iniciativas políticas

³² Reglamento (UE) n.º 580/2011 del Parlamento Europeo y del Consejo, de 8 de junio de 2011, que modifica el Reglamento (CE) n.º 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, en lo que respecta a su duración (DO L 165 de 24.6.2011, p. 3).

³³ Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004 (DO L 165 de 18.6.2013, p. 41).

sectoriales de la Unión en lo que respecta a la ciberseguridad y fomentando la cooperación operativa entre los Estados miembros, así como entre los Estados miembros y las instituciones, órganos y organismos de la UE.

- (10) En el marco de la Decisión 2004/97/CE, Euratom, adoptada en la reunión del Consejo Europeo celebrada el 13 de diciembre de 2003, los representantes de los Estados miembros decidieron que ENISA tendría su sede en una ciudad de Grecia que determinaría el Gobierno griego. El Estado miembro que acoge a la Agencia debe ofrecer las mejores condiciones posibles para un funcionamiento fluido y eficaz de la misma. Para el desempeño correcto y eficaz de sus funciones, para atraer y conservar al personal y para facilitar el establecimiento de contactos con el exterior, es necesario que la Agencia tenga su sede en un lugar adecuado que, entre otras cosas, ofrezca conexiones de transporte adecuadas y servicios para los cónyuges y los hijos que acompañen a su personal. Las disposiciones necesarias deben recogerse en un acuerdo entre la Agencia y el Estado miembro anfitrión, cuya celebración ha de contar con la aprobación del Consejo de Administración de la Agencia.
- (11) En vista de los crecientes retos en materia de ciberseguridad a que se enfrenta la Unión, deben incrementarse los recursos financieros y humanos asignados a la Agencia, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crítica en el ecosistema de organizaciones que defienden el ecosistema digital europeo.
- (12) La Agencia debe desarrollar y mantener un elevado nivel de conocimientos técnicos y actuar como punto de referencia que genere confianza en el mercado único en virtud de su independencia, la calidad del asesoramiento prestado y la información difundida, la transparencia de sus procedimientos y métodos de funcionamiento y su diligencia en el desempeño de sus tareas. La Agencia debe contribuir proactivamente a los esfuerzos nacionales y de la Unión y desempeñar sus funciones cooperando plenamente con las instituciones, órganos y organismos de la Unión y los Estados miembros. Además, la Agencia debe apoyarse en las aportaciones del sector privado y en la cooperación con el mismo, así como con otras partes interesadas pertinentes. Debe existir un conjunto de funciones que establezca cómo debe alcanzar la Agencia sus objetivos, pero permita cierta flexibilidad en su funcionamiento.
- (13) La Agencia debe prestar asistencia a la Comisión mediante asesoramiento, dictámenes y análisis en todos los asuntos de la Unión relacionados con la formulación de políticas y disposiciones legislativas, actualizaciones y revisiones en el ámbito de la ciberseguridad, con inclusión de la protección de infraestructuras críticas y la ciberresiliencia. La Agencia debe actuar como punto de referencia de asesoramiento y conocimientos para la política y las iniciativas legislativas sectoriales de la Unión, cuando intervengan cuestiones relacionadas con la ciberseguridad.
- (14) El cometido subyacente de la Agencia es promover la aplicación coherente del marco jurídico pertinente, en particular la aplicación efectiva de la Directiva SRI, que es esencial para aumentar la ciberresiliencia. Habida cuenta de la constante evolución de las amenazas para la ciberseguridad, es evidente que los Estados miembros deben estar respaldados por un enfoque más global y transversal en lo que se refiere a la creación de ciberresiliencia.
- (15) La Agencia debe asistir a los Estados miembros y a las instituciones, órganos y organismos de la Unión en sus esfuerzos por conformar y mejorar su capacidad y preparación para prevenir, detectar y dar respuesta a los problemas e incidentes de ciberseguridad, así como en relación con la seguridad de las redes y los sistemas de

información. En particular, la Agencia debe prestar apoyo al desarrollo y potenciación de los CSIRT nacionales, con vistas a que alcancen un elevado nivel común de madurez en la Unión. La Agencia debe también prestar asistencia en la elaboración y actualización de las estrategias de los Estados miembros y de la Unión en materia de seguridad de las redes y los sistemas de información, y en particular de ciberseguridad, promover su difusión y hacer un seguimiento de los avances en su aplicación. La Agencia debe ofrecer asimismo cursos y material de formación a los organismos públicos y, cuando proceda, «formar formadores» con el fin de ayudar a los Estados miembros a desarrollar sus propias capacidades de formación.

- (16) La Agencia debe asistir al Grupo de cooperación establecido en la Directiva SRI en la ejecución de sus tareas, en particular ofreciendo asesoramiento y consejo y facilitando el intercambio de mejores prácticas, particularmente con respecto a la identificación de los operadores de servicios esenciales por parte de los Estados miembros, en especial en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes.
- (17) Con el fin de estimular la cooperación entre los sectores público y privado y dentro del sector privado, y en particular para apoyar la protección de las infraestructuras críticas, la Agencia debe facilitar la creación de centros sectoriales de puesta en común y análisis de la información (ISAC, por sus siglas en inglés), proporcionando directrices y mejores prácticas sobre las herramientas disponibles y los procedimientos, y orientando sobre la manera de abordar los asuntos normativos relacionados con la puesta en común de la información.
- (18) La Agencia debe agregar y analizar los informes nacionales de los CSIRT y el CERT-UE y establecer unas normas, un lenguaje y una terminología comunes para el intercambio de información. Debe también fomentar la participación del sector privado, en el marco de la Directiva SRI, que estableció las bases para el intercambio voluntario de información técnica a nivel operativo con la creación de la red de CSIRT.
- (19) La Agencia debe contribuir a aportar una respuesta a nivel de la UE en caso de incidentes y crisis de ciberseguridad transfronterizas a gran escala. Esta función debe incluir la recogida de información pertinente y el desempeño del papel de mediador entre la red de CSIRT y la comunidad técnica, así como los responsables políticos de gestionar la crisis. Por otra parte, la Agencia podría apoyar la gestión de incidentes desde una perspectiva técnica facilitando el intercambio de soluciones técnicas pertinentes entre los Estados miembros y aportando información a las comunicaciones públicas. La Agencia debe apoyar el proceso ensayando modalidades de esta cooperación a través de ejercicios anuales de ciberseguridad.
- (20) Para llevar a cabo sus tareas operativas, la Agencia debe hacer uso de las competencias disponibles del CERT-UE a través de una cooperación estructurada, en estrecha proximidad física. La cooperación estructurada facilitará las sinergias necesarias y permitirá acumular conocimientos a ENISA. Cuando proceda, deben establecerse disposiciones específicas adecuadas entre las dos organizaciones para definir los aspectos prácticos de dicha cooperación.
- (21) En cumplimiento de sus tareas operativas, la Agencia debe poder prestar ayuda a los Estados miembros, por ejemplo, mediante asesoramiento, asistencia técnica o análisis de amenazas e incidentes. La Recomendación de la Comisión sobre la respuesta coordinada a las crisis e incidentes de ciberseguridad a gran escala recomienda que los Estados miembros cooperen de buena fe y compartan entre ellos y con ENISA

información sobre las crisis e incidentes de ciberseguridad a gran escala sin demora indebida. Dicha información debe servir de ayuda a ENISA en el desempeño de sus funciones operativas.

- (22) Dentro de la cooperación regular a nivel técnico para ayudar a la Unión a conocer la situación, la Agencia debe elaborar periódicamente el informe técnico de ciberseguridad de la UE sobre incidentes y amenazas, basándose en la información públicamente disponible, en su propio análisis y en los informes compartidos por los CSIRT de los Estados miembros (voluntariamente) o los puntos de contacto únicos de la Directiva SRI, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y, cuando proceda, el Centro de Inteligencia de la Unión Europea (INTCEN) del Servicio Europeo de Acción Exterior (SEAE). El informe debe ponerse a disposición de las instancias pertinentes del Consejo, la Comisión, la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y la red de CSIRT.
- (23) Las investigaciones técnicas *ex post* en relación con incidentes con efectos significativos en más de un Estado miembro respaldadas o efectuadas por la Agencia a petición o con el acuerdo de los Estados miembros afectados deben centrarse en la prevención de incidentes futuros y llevarse a cabo sin perjuicio de eventuales procedimientos judiciales o administrativos destinados a determinar culpas o responsabilidades.
- (24) Los Estados miembros afectados deben proporcionar a la Agencia la información y asistencia necesarias a efectos de la investigación, sin perjuicio de lo dispuesto en el artículo 346 del Tratado de Funcionamiento de la Unión Europea u otras razones de interés público.
- (25) Los Estados miembros podrán invitar a las empresas afectadas por el incidente a colaborar facilitando a la Agencia toda la información y asistencia necesarias, sin perjuicio de su derecho a proteger la información sensible desde el punto de vista comercial.
- (26) Para comprender mejor los retos en el campo de la ciberseguridad, y con el fin de facilitar asesoramiento estratégico a largo plazo a los Estados miembros y las instituciones de la Unión, la Agencia necesita analizar los riesgos actuales y emergentes. A tal efecto, la Agencia, en cooperación con los Estados miembros y, si procede, con los organismos estadísticos o de otro tipo, debe recopilar la información pertinente y llevar a cabo análisis de las tecnologías emergentes y proporcionar evaluaciones temáticas sobre los efectos jurídicos, económicos, sociales y reglamentarios que se esperan de las innovaciones tecnológicas sobre la seguridad de las redes y de la información, en particular la ciberseguridad. Además, la Agencia debe apoyar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a la hora de detectar nuevas tendencias y prevenir los problemas relacionados con la ciberseguridad, mediante la realización de análisis de amenazas e incidentes.
- (27) Con el fin de aumentar la resiliencia de la Unión, la Agencia debe desarrollar la excelencia en el ámbito de la seguridad de la infraestructura de internet y de las infraestructuras críticas, ofreciendo asesoramiento, directrices y mejores prácticas. Con el fin de facilitar el acceso a una información mejor estructurada sobre los riesgos para la ciberseguridad y las posibles soluciones, la Agencia debe crear y mantener la «plataforma de información» de la Unión, un portal único con información sobre ciberseguridad para los ciudadanos procedente de las instituciones, órganos y organismos nacionales y de la UE.

- (28) La Agencia debe contribuir a la sensibilización del público sobre los riesgos para la ciberseguridad y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos y organizaciones. Debe contribuir asimismo a promover las mejores prácticas y soluciones a nivel de personas y organizaciones mediante la recogida y análisis de la información disponible públicamente relativa a incidentes significativos y la elaboración de informes con vistas a ofrecer orientaciones a empresas y ciudadanos y mejorar el nivel general de preparación y resiliencia. La Agencia debe además, en colaboración con los Estados miembros y las instituciones, órganos y organismos de la Unión, organizar campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y a concienciar sobre las amenazas potenciales en el ciberespacio, incluyendo ciberdelitos como los ataques por suplantación de identidad (*phishing*), las redes infectadas (*botnets*) o los fraudes bancarios y financieros, así como dar consejos básicos en materia de autenticación y protección de datos. La Agencia debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos.
- (29) Con el fin de apoyar a las empresas que trabajan en el sector de la ciberseguridad, así como a los usuarios de soluciones de ciberseguridad, la Agencia debe crear y mantener un «observatorio del mercado», llevando a cabo análisis y difundiendo las principales tendencias en el mercado de la ciberseguridad, tanto en el lado de la oferta como en el de la demanda.
- (30) Para asegurar que cumple plenamente sus objetivos, la Agencia debe permanecer en contacto con las instituciones, órganos y organismos pertinentes, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Agencia Europea de Defensa (AED), la Agencia europea para la gestión operativa de los sistemas informáticos de gran magnitud (eu-LISA), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la UE relacionado con la ciberseguridad. También debe mantener contactos con las autoridades encargadas de la protección de datos a fin de intercambiar conocimientos y mejores prácticas y facilitar asesoramiento sobre los aspectos de la ciberseguridad que podrían repercutir en su trabajo. Los representantes de las autoridades nacionales y de la Unión encargadas de hacer cumplir la ley y proteger los datos deben poder estar representados en el Grupo Permanente de Partes Interesadas de la Agencia. En sus relaciones con los organismos encargados de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en el trabajo de dichos organismos, la Agencia debe respetar los canales de información y las redes existentes.
- (31) La Agencia, como miembro de la red de CSIRT que además se encarga de su secretaría, debe prestar apoyo a los CSIRT de los Estados miembros y al CERT-UE en la cooperación operativa relativa a todas las tareas pertinentes de la red de CSIRT, tal como se definen en la Directiva SRI. Además, la Agencia debe promover y apoyar la cooperación entre los CSIRT pertinentes en caso de incidentes, ataques o perturbaciones en las redes o infraestructuras gestionadas o protegidas por los CSIRT y que impliquen o puedan implicar al menos a dos CERT, teniendo siempre debidamente en cuenta los procedimientos operativos estándar de la red de CSIRT.
- (32) Con el fin de aumentar la preparación de la Unión para una respuesta a los incidentes de ciberseguridad, la Agencia debe organizar anualmente ejercicios de ciberseguridad a nivel de la Unión y, cuando lo soliciten, apoyar a los Estados miembros y las instituciones, órganos y organismos de la UE en la organización de ejercicios.

- (33) La Agencia debe desarrollar y mantener sus conocimientos técnicos en materia de certificación de la ciberseguridad con vistas a respaldar la política de la Unión en este ámbito. Debe igualmente promover la asimilación de la certificación de la ciberseguridad en la Unión, en particular contribuyendo a la creación y mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.
- (34) Unas políticas de ciberseguridad eficientes deben basarse en métodos de evaluación de riesgos bien desarrollados, tanto en el sector público como en el privado. Los métodos de evaluación de riesgos se utilizan en distintos niveles sin que existan prácticas comunes para su aplicación eficiente. La promoción y el desarrollo de las mejores prácticas de evaluación de riesgos y de soluciones interoperables de gestión de riesgos en las organizaciones de los sectores público y privado incrementarán el nivel de ciberseguridad en la Unión. A tal efecto, la Agencia debe apoyar la cooperación entre las partes interesadas a escala de la Unión, facilitando sus esfuerzos en relación con el establecimiento y la adopción de normas a escala europea e internacional para la gestión del riesgo y la seguridad mensurable de los productos, sistemas, redes y servicios electrónicos que, junto a los programas informáticos, conforman las redes y los sistemas de información.
- (35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ciberseguridad personal. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ciberseguridad. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ciberseguridad de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ciberseguridad, de sus productos y servicios.
- (36) La Agencia debe tener plenamente en cuenta las actividades en curso de investigación, desarrollo y evaluación tecnológica, en especial las llevadas a cabo por las distintas iniciativas de investigación de la Unión, para asesorar a las instituciones, órganos y organismos de la Unión y, cuando proceda, a los Estados miembros que lo soliciten sobre las necesidades de investigación en el ámbito de la seguridad de las redes y de la información, y en particular de la ciberseguridad.
- (37) Los problemas de ciberseguridad tienen un alcance mundial. Es necesaria una cooperación internacional más estrecha para mejorar las normas de seguridad, incluida la definición de normas de comportamiento comunes, y el intercambio de información, promoviendo una colaboración internacional que responda con mayor prontitud a los problemas de seguridad de las redes y de la información, así como un enfoque mundial común al respecto. A tal efecto, la Agencia debe respaldar una mayor relación y cooperación de la Unión con los terceros países y las organizaciones internacionales proporcionando, cuando proceda, los conocimientos y el análisis necesarios a las instituciones, órganos y organismos pertinentes de la Unión.
- (38) La Agencia debe estar en condiciones de responder a las solicitudes específicas de asesoramiento y asistencia por parte de los Estados miembros y las instituciones, órganos y organismos de la UE que cuadren con los objetivos de la Agencia.

- (39) Es necesario aplicar determinados principios al gobierno de la Agencia con el fin de atenerse a la declaración conjunta y el enfoque común aprobados en julio de 2012 por el Grupo de trabajo interinstitucional sobre las agencias descentralizadas, declaración y enfoque cuya finalidad es la racionalización las actividades de las agencias y la mejora de su rendimiento. La declaración conjunta y el enfoque común también han de quedar reflejados, cuando proceda, en los programas de trabajo de la Agencia, sus evaluaciones y sus prácticas administrativas y de presentación de informes.
- (40) El Consejo de Administración, integrado por los Estados miembros y la Comisión, debe definir la orientación general del funcionamiento de la Agencia y garantizar que desempeña su cometido de conformidad con el presente Reglamento. El Consejo de Administración debe estar dotado de las facultades necesarias para establecer el presupuesto, supervisar su ejecución, aprobar el correspondiente reglamento financiero, establecer procedimientos de trabajo transparentes para la toma de decisiones por la Agencia, adoptar el documento único de programación de la Agencia, adoptar su propio reglamento interno, nombrar al director ejecutivo y decidir la prolongación del mandato del director ejecutivo o el cese de dicho mandato.
- (41) Para que la Agencia funcione correcta y eficazmente, la Comisión y los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales adecuadas y de experiencia en las áreas funcionales. La Comisión y los Estados miembros deben asimismo tratar de limitar la rotación de sus respectivos representantes en el Consejo de Administración, con el fin de garantizar la continuidad en su labor.
- (42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ciberseguridad. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia, previa consulta con la Comisión, y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe tener la posibilidad de crear grupos de trabajo *ad hoc* para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo *ad hoc* sean seleccionados entre los expertos de mayor nivel, teniendo debidamente en cuenta la necesidad de lograr un equilibrio representativo, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información.
- (43) El Comité Ejecutivo debe contribuir al buen funcionamiento del Consejo de Administración. Como parte de sus trabajos preparatorios relativos a las decisiones del Consejo de Administración, debe examinar en detalle la información pertinente, explorar las opciones disponibles y ofrecer asesoramiento y soluciones para preparar las decisiones pertinentes del Consejo de Administración.
- (44) La Agencia debe contar con un Grupo Permanente de Partes Interesadas en calidad de organismo consultivo, a fin de garantizar un diálogo sistemático con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes. El Grupo

Permanente de Partes Interesadas, establecido por el Consejo de Administración a propuesta del director ejecutivo, debe centrarse en cuestiones que afecten a las partes interesadas y ponerlas en conocimiento de la Agencia. La composición del Grupo Permanente de Partes Interesadas y las tareas asignadas a este grupo, que debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo, deben garantizar una representación suficiente de las partes interesadas en los trabajos de la Agencia.

- (45) La Agencia instaurará normas para la prevención y gestión de los conflictos de intereses. La Agencia debe aplicar asimismo las disposiciones pertinentes de la Unión relativas al acceso del público a los documentos, según establece el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo³⁴. Los datos personales deben ser tratados por la Agencia de conformidad con el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos³⁵. La Agencia 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 sensible no clasificada y la información clasificada de la UE.
- (46) Con el fin de garantizar la plena autonomía e independencia de la Agencia y para que pueda desempeñar funciones adicionales y nuevas, incluidas tareas de emergencia imprevistas, se considera necesario concederle un presupuesto suficiente y autónomo cuyos ingresos procedan principalmente de una contribución de la Unión y de contribuciones de los terceros países que participen en los trabajos de la Agencia. La mayor parte del personal de la Agencia debe estar dedicado directamente a la aplicación operativa de su mandato. Debe permitirse que el Estado miembro que la acoge, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de la Agencia. El procedimiento presupuestario de la Unión debe seguir siendo aplicable por lo que respecta a las subvenciones imputables al presupuesto general de la Unión. Además, el Tribunal de Cuentas Europeo debe realizar una auditoría de las cuentas de la Agencia para garantizar la transparencia y la responsabilidad.
- (47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

³⁴ 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).

³⁵ DO L 8 de 12.1.2001, p. 1.

- (48) La certificación de la ciberseguridad desempeña un importante papel a la hora de aumentar la confianza y la seguridad en los productos y servicios de TIC. El mercado único digital, y en particular la economía de los datos y la internet de las cosas, solo pueden prosperar si el público en general confía en que dichos productos y servicios ofrecen un determinado nivel de garantía de ciberseguridad. Los vehículos conectados y automatizados, los dispositivos médicos electrónicos, los sistemas de control de la automatización industrial o las redes inteligentes son solo algunos ejemplos de sectores en los que la certificación se utiliza ya ampliamente o es probable que se utilice en un futuro próximo. También en los sectores regulados por la Directiva SRI resulta crítica la certificación de la ciberseguridad.
- (49) En la Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora», la Comisión indicó la necesidad de productos y soluciones de ciberseguridad de alta calidad, asequibles e interoperables. El suministro de los productos y servicios de TIC dentro del mercado único sigue estando muy fragmentado desde el punto de vista geográfico. Esto se debe a que la industria de la ciberseguridad en Europa se ha desarrollado en gran medida a partir de la demanda de los gobiernos nacionales. Además, la falta de soluciones interoperables (normas técnicas), prácticas y mecanismos de certificación a escala de la UE es otra de las carencias que padece el mercado único de la ciberseguridad. Por una parte, esto hace difícil que las empresas europeas compitan a nivel nacional, europeo y mundial; por otra, reduce las opciones de contar con tecnologías de ciberseguridad viables y utilizables a las que puedan acceder particulares y empresas. Del mismo modo, en la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, la Comisión destacó la necesidad de seguridad en los productos y sistemas conectados, indicando que la creación de un marco europeo de seguridad de las TIC que establezca pautas para organizar la certificación de seguridad de las TIC en la Unión podría tanto preservar la confianza en internet como combatir la actual fragmentación del mercado de la ciberseguridad.
- (50) En la actualidad, la certificación de la ciberseguridad de los productos y servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real.
- (51) Se han realizado esfuerzos en el pasado para propiciar el reconocimiento mutuo de los certificados en Europa, pero solo han tenido un éxito parcial. El ejemplo más importante a este respecto es el Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS). Si bien constituye el modelo más importante para la cooperación y el reconocimiento mutuo en el ámbito de la certificación de la seguridad, el ARM del SOG-IS presenta algunas deficiencias importantes relacionadas con su elevado coste y limitado alcance. Hasta la fecha, solo se ha desarrollado un corto número de perfiles de protección para

productos digitales tales como la firma digital, el tacógrafo digital y las tarjetas inteligentes. Y lo que es más importante, el SOG-IS incluye solo a una parte de los Estados miembros de la Unión. Esto ha limitado la eficacia del ARM del SOG-IS desde el punto de vista del mercado interior.

- (52) Por todo ello, es necesario establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar regímenes europeos de certificación de la ciberseguridad y permita que los certificados de productos y servicios de TIC sean reconocidos y usados en todos los Estados miembros. El marco europeo debe tener un doble objetivo: por una parte, contribuir a aumentar la confianza en los productos y servicios de TIC que hayan sido certificados con arreglo a tales regímenes; por otra, evitar la multiplicación de certificaciones nacionales de la ciberseguridad contradictorias o redundantes y, por ende, reducir los costes para las empresas que operan en el mercado único digital. Los regímenes deben ser no discriminatorios y basarse en normas internacionales o de la Unión, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la UE al respecto.
- (53) La Comisión debe estar facultada para adoptar regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del Reglamento. No obstante, los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos.
- (54) Las disposiciones del presente Reglamento deben entenderse sin perjuicio de la legislación de la Unión que fija normas específicas sobre la certificación de productos y servicios de TIC. En particular, el Reglamento general de protección de datos (RGPD) establece disposiciones para implantar mecanismos de certificación y sellos y marcas de protección de datos a fin de demostrar la conformidad con ese Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. Estos mecanismos de certificación y sellos y marcas de protección de datos deben permitir a los interesados evaluar rápidamente el nivel de protección de datos de los correspondientes productos y servicios. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del RGPD, incluso cuando dichas operaciones se encuentran integradas en productos y servicios.
- (55) El objetivo de los regímenes europeos de certificación de la ciberseguridad debe ser garantizar que los productos y servicios de TIC certificados con arreglo a un régimen cumplan los requisitos especificados. Tales requisitos se refieren a la capacidad de resistir, con un nivel determinado de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, procesos, servicios y sistemas, en el sentido del presente Reglamento, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle en el presente Reglamento los requisitos de ciberseguridad relativos a todos los productos y servicios de TIC. Los productos y servicios de TIC y las correspondientes necesidades de ciberseguridad son tan dispares que es muy difícil presentar unos requisitos de ciberseguridad generales de validez global. Por lo tanto, es necesario adoptar un

concepto amplio y general de la ciberseguridad a efectos de la certificación, complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los regímenes europeos de certificación de la ciberseguridad. Las modalidades con que se lograrán tales objetivos para determinados productos y servicios de TIC deben especificarse luego con más detalle a nivel de cada régimen de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas.

- (56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. A continuación, la Comisión, sobre la base de las propuestas presentadas por ENISA, debe estar facultada para adoptar el régimen europeo de certificación de la ciberseguridad mediante actos de ejecución. Teniendo en cuenta la finalidad general y los objetivos de seguridad definidos en el presente Reglamento, los regímenes europeos de certificación de la ciberseguridad adoptados por la Comisión deben especificar un conjunto mínimo de elementos relacionados con el objeto, alcance y funcionamiento del régimen concreto. Entre ellos deben figurar el alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos y servicios de TIC que cubre, la especificación detallada de los requisitos de ciberseguridad, por ejemplo haciendo referencia a normas o especificaciones técnicas, los criterios y métodos de evaluación específicos, así como el nivel de garantía: básico, sustancial o elevado.
- (57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.
- (58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.
- (59) Es necesario exigir a todos los Estados miembros que designen a una autoridad de supervisión de la certificación de la ciberseguridad para supervisar el cumplimiento, por parte de los organismos de evaluación de la conformidad establecidos en su territorio y de los certificados por ellos expedidos, de los requisitos del presente Reglamento y de los regímenes de certificación de la ciberseguridad pertinentes. Las autoridades nacionales de supervisión de la certificación deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los

certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigar el asunto objeto de la reclamación en la medida que proceda e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable. Además, deben cooperar con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes de ciberseguridad específicos.

- (60) Con vistas a garantizar una aplicación coherente del marco europeo de certificación de la ciberseguridad, debe establecerse un Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»), constituido por las autoridades nacionales de supervisión de la certificación. Los cometidos principales del Grupo deben ser asesorar y asistir a la Comisión en su labor de garantizar una implantación y aplicación coherentes del marco europeo de certificación de la ciberseguridad; asistir y cooperar estrechamente con la Agencia en la preparación de las propuestas de regímenes de certificación de la ciberseguridad; recomendar que la Comisión solicite a la Agencia que prepare una propuesta de régimen europeo de certificación de la ciberseguridad; y adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los regímenes europeos de certificación de la ciberseguridad existentes.
- (61) Con el fin de reforzar la sensibilización y facilitar la aceptación de los futuros regímenes de ciberseguridad de la UE, la Comisión Europea podrá formular directrices generales o sectoriales en materia de ciberseguridad, por ejemplo, sobre buenas prácticas de ciberseguridad o sobre comportamiento responsable en materia de ciberseguridad, destacando el efecto positivo de la utilización de productos y servicios TIC certificados.
- (62) La ayuda prestada por la Agencia a la certificación de la ciberseguridad debe incluir también los contactos con el Comité de Seguridad del Consejo y el organismo nacional pertinente, en relación con la aprobación criptográfica de los productos para su uso en redes clasificadas.
- (63) A fin de precisar los criterios para la acreditación de los organismos de evaluación de la conformidad, deben delegarse en la Comisión los poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. La Comisión debe llevar a cabo las oportunas consultas durante sus trabajos preparatorios, también a nivel de expertos. Dichas consultas deben realizarse de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016. En particular, para garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.
- (64) A fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011.
- (65) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los regímenes europeos de certificación de la ciberseguridad de productos y

servicios de TIC, sobre las modalidades de ejecución de las investigaciones por parte de la Agencia y sobre las circunstancias, formatos y procedimientos de notificación a la Comisión por parte de los organismos de evaluación de la conformidad acreditados por las autoridades nacionales de supervisión de la certificación.

- (66) Las actividades de la Agencia deben evaluarse de modo independiente. La evaluación debe tener en cuenta el logro de sus objetivos por parte de la Agencia, sus prácticas de trabajo y la pertinencia de sus tareas. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad.
- (67) Procede derogar el Reglamento (UE) n.º 526/2013.
- (68) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que pueden lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

Con vistas a garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, el presente Reglamento:

- a) establece los objetivos, funciones y aspectos organizativos de ENISA, la «Agencia de Ciberseguridad de la UE», denominada en lo sucesivo «la Agencia»; y
- b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

- 1) «ciberseguridad», todas las actividades necesarias para la protección de las redes y sistemas de información, de sus usuarios y de las personas afectadas por las ciberamenazas;
- 2) «redes y sistemas de información», un sistema en el sentido del artículo 4, punto 1, de la Directiva (UE) 2016/1148;
- 3) «estrategia nacional de seguridad de las redes y sistemas de información», un marco en el sentido del artículo 4, punto 3, de la Directiva (UE) 2016/1148;
- 4) «operador de servicios esenciales», una entidad pública o privada según se define en el artículo 4, punto 4, de la Directiva (UE) 2016/1148;
- 5) «proveedor de servicios digitales», una persona jurídica que presta un servicio digital según se define en el artículo 4, punto 6, de la Directiva (UE) 2016/1148;
- 6) «incidente», un hecho según se define en el artículo 4, punto 7, de la Directiva (UE) 2016/1148;
- 7) «gestión de incidentes», un procedimiento según se define en el artículo 4, punto 8, de la Directiva (UE) 2016/1148;
- 8) «ciberamenaza», cualquier circunstancia potencial o hecho que pueda afectar desfavorablemente a las redes y los sistemas de información, a sus usuarios y a las personas afectadas;
- 9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos y servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico;

- 10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad;
- 11) «producto y servicio de TIC», todo elemento o grupo de elementos de las redes y los sistemas de información;
- 12) «acreditación», una acreditación tal como se define en el artículo 2, punto 10, del Reglamento (CE) n.º 765/2008;
- 13) «organismo nacional de acreditación», un organismo nacional de acreditación tal como se define en el artículo 2, punto 11, del Reglamento (CE) n.º 765/2008;
- 14) «evaluación de la conformidad», la evaluación de la conformidad tal como se define en el artículo 2, punto 12, del Reglamento (CE) n.º 765/2008;
- 15) «organismo de evaluación de la conformidad», el organismo de evaluación de la conformidad tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008;
- 16) «norma», una norma según se define en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012.

TÍTULO II

ENISA – la «Agencia de Ciberseguridad de la UE»

CAPÍTULO I

MANDATO, OBJETIVOS Y TAREAS

Artículo 3

Mandato

1. La Agencia desempeñará los cometidos que le asigna el presente Reglamento con el fin de contribuir a un elevado nivel de ciberseguridad dentro de la Unión.
2. La Agencia desempeñará los cometidos que le confieran los actos de la Unión que establecen medidas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de ciberseguridad.
3. Los objetivos y cometidos de la Agencia se entenderán sin perjuicio de las competencias de los Estados miembros en materia de ciberseguridad y, en todo caso, sin perjuicio de las actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

Artículo 4

Objetivos

1. La Agencia será un centro de conocimientos técnicos sobre ciberseguridad en virtud de su independencia, la calidad científica y técnica del asesoramiento y la asistencia prestados y la información ofrecida, la transparencia de sus procedimientos operativos y métodos de funcionamiento y su diligencia en el desempeño de sus funciones.
2. La Agencia asistirá a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas relativas a la ciberseguridad.
3. La Agencia prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a la Unión, los Estados miembros y las partes interesadas públicas y privadas a fin de incrementar la protección de sus redes y sistemas de información, desarrollar las capacidades y competencias en el ámbito de la ciberseguridad y lograr la ciberresiliencia.
4. La Agencia fomentará la cooperación y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, incluido el sector privado, sobre las cuestiones relacionadas con la ciberseguridad.
5. La Agencia incrementará las capacidades de ciberseguridad a nivel de la Unión para complementar la acción de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.
6. La Agencia promoverá el uso de la certificación, en particular contribuyendo a la creación y el mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión de conformidad con el título III del presente Reglamento, con el fin de

aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.

7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad.

Artículo 5

Tareas relativas al desarrollo y ejecución de la política y la legislación de la Unión

La Agencia contribuirá al desarrollo y ejecución de la política y la legislación de la Unión:

1. Prestando asistencia y asesoramiento, en particular emitiendo su dictamen independiente y aportando trabajos preparatorios, en el desarrollo y la revisión de la política y la legislación de la Unión en el ámbito de la ciberseguridad, así como las iniciativas políticas y legislativas sectoriales cuando estén presentes cuestiones relacionadas con la ciberseguridad.
2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y la legislación de la Unión en materia de ciberseguridad, especialmente en relación con la Directiva (UE) 2016/1148, en particular a través de dictámenes, directrices, recomendaciones y mejores prácticas sobre temas como la gestión de riesgos, la notificación de incidentes y la comunicación de información, así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto.
3. Contribuyendo a los trabajos del Grupo de cooperación con arreglo al artículo 11 de la Directiva (UE) 2016/1148, ofreciendo su asesoramiento y asistencia.
4. Respalando:
 - 1) el desarrollo y la aplicación de la política de la Unión en el ámbito de la identidad electrónica y los servicios de confianza, en particular ofreciendo asesoramiento y directrices técnicas y facilitando el intercambio de mejores prácticas entre las autoridades competentes;
 - 2) la promoción de una mejora del nivel de seguridad de las comunicaciones electrónicas, en particular ofreciendo asistencia y asesoramiento y facilitando el intercambio de mejores prácticas entre las autoridades competentes.
5. Respalando la revisión periódica de las actividades políticas de la Unión mediante la preparación de un informe anual sobre el estado de la aplicación del marco jurídico respectivo en relación con:
 - a) las notificaciones de incidentes de los Estados miembros suministradas por el punto de contacto único al Grupo de cooperación de conformidad con el artículo 10, apartado 3, de la Directiva (UE) 2016/1148;
 - b) las notificaciones de violación de la seguridad y pérdida de la integridad respecto de los proveedores de servicios de confianza, suministradas por los organismos de supervisión a la Agencia de conformidad con el artículo 19, apartado 3, del Reglamento (UE) n.º 910/2014;
 - c) las notificaciones de violación de la seguridad transmitidas por las empresas suministradoras de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, suministradas por las

autoridades competentes a la Agencia de conformidad con el artículo 40 de la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas].

Artículo 6

Tareas relativas a la creación de capacidades

1. La Agencia asistirá:
 - a) a los Estados miembros en sus esfuerzos por mejorar la prevención, detección, análisis y capacidad de respuesta a problemas e incidentes de ciberseguridad, proporcionándoles los conocimientos teóricos y prácticos necesarios;
 - b) a las instituciones, órganos y organismos de la Unión en sus esfuerzos para mejorar la prevención, detección, análisis y capacidad de respuesta a problemas e incidentes de ciberseguridad a través de un apoyo adecuado al CERT de las instituciones, órganos y organismos de la Unión (CERT-UE);
 - c) a los Estados miembros, a petición suya, en el desarrollo de equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), con arreglo al artículo 9, apartado 5, de la Directiva (UE) 2016/1148;
 - d) a los Estados miembros, a petición suya, en el desarrollo de estrategias nacionales sobre seguridad de las redes y los sistemas de información, con arreglo al artículo 7, apartado 2, de la Directiva (UE) 2016/1148; la Agencia también promoverá la difusión y el seguimiento de los progresos en la aplicación de estas estrategias en toda la Unión, con el fin de promover las mejores prácticas;
 - e) a las instituciones de la Unión en la elaboración y revisión de las estrategias de la Unión en materia de ciberseguridad, promoviendo la difusión y el seguimiento de los progresos en su aplicación;
 - f) a los CSIRT nacionales y de la Unión para elevar el nivel de sus capacidades, en particular promoviendo el diálogo y el intercambio de información, con el fin de lograr que, habida cuenta de los avances más recientes, cada CSIRT disponga de un conjunto mínimo de capacidades y se atenga a las mejores prácticas;
 - g) a los Estados miembros, organizando cada año los ejercicios de ciberseguridad a gran escala a nivel de la Unión a que se refiere el artículo 7, apartado 6, y formulando recomendaciones políticas basadas en el proceso de evaluación de los ejercicios y en las enseñanzas extraídas de ellos;
 - h) a los organismos públicos pertinentes, ofreciendo formación sobre ciberseguridad, en colaboración, cuando proceda, con las partes interesadas;
 - i) al Grupo de cooperación, mediante el intercambio de mejores prácticas, en particular con respecto a la identificación de los operadores de servicios esenciales por parte de los Estados miembros, especialmente en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes, con arreglo al artículo 11, apartado 3, letra l), de la Directiva (UE) 2016/1148.
2. La Agencia facilitará el establecimiento de centros sectoriales de puesta en común y análisis de la información (ISAC) y les prestará un apoyo continuado, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, aportando

mejores prácticas y orientaciones sobre las herramientas disponibles, el procedimiento y la manera de abordar los asuntos normativos relacionados con el intercambio de información.

Artículo 7

Tareas relativas a la cooperación operativa a nivel de la Unión

1. La Agencia apoyará la cooperación operativa entre los organismos públicos competentes y entre las partes interesadas.
2. La Agencia cooperará a nivel operativo y establecerá sinergias con las instituciones, órganos y organismos de la Unión, incluido el CERT-UE, los servicios que abordan la ciberdelincuencia y las autoridades responsables de la protección de la intimidad y los datos personales, con vistas a tratar cuestiones de interés común, en particular mediante:
 - a) el intercambio de conocimientos técnicos y mejores prácticas;
 - b) la prestación de asesoramiento y directrices sobre cuestiones de interés relacionadas con la ciberseguridad;
 - c) el establecimiento, previa consulta de la Comisión, de disposiciones prácticas para la ejecución de tareas específicas.
3. La Agencia se hará cargo de la secretaría de la red de CSIRT, de conformidad con el artículo 12, apartado 2, de la Directiva (UE) 2016/1148, y facilitará activamente el intercambio de información y la cooperación entre sus miembros.
4. La Agencia contribuirá a la cooperación operativa dentro de la red de CSIRT y prestará apoyo a los Estados miembros:
 - a) asesorando sobre cómo mejorar su capacidad para prevenir, detectar y dar respuesta a los incidentes;
 - b) proporcionando, previa solicitud, asistencia técnica en caso de incidentes con un impacto significativo o sustancial;
 - c) analizando las vulnerabilidades, artefactos e incidentes.

En el desempeño de estas funciones, la Agencia y el CERT-UE entablarán una cooperación estructurada con el fin de beneficiarse de las sinergias, especialmente en lo que se refiere a los aspectos operativos.

5. A petición de dos o más Estados miembros afectados y con el único objetivo de prestar asesoramiento para la prevención de incidentes futuros, la Agencia prestará apoyo para que se realice, o realizará, una investigación técnica *ex post* tras las notificaciones por las empresas afectadas de incidentes que tengan un impacto significativo o sustancial con arreglo a la Directiva (UE) 2016/1148. La Agencia también llevará a cabo dicha investigación tras una solicitud debidamente justificada de la Comisión de acuerdo con los Estados miembros afectados en caso de incidentes que afecten a más de dos Estados miembros.

El alcance de la investigación y el procedimiento que debe seguirse para llevarla a cabo serán objeto de acuerdo entre los Estados miembros afectados y la Agencia, y se entenderá sin perjuicio de eventuales investigaciones penales relativas al mismo incidente. La investigación concluirá con un informe técnico final elaborado por la Agencia, en particular sobre la base de la información y las observaciones de los Estados miembros y empresa(s) afectados y consensuado con los Estados miembros afectados. Se ofrecerá a la red de CSIRT un resumen del informe centrado en las recomendaciones para la prevención de incidentes futuros.

6. La Agencia organizará anualmente ejercicios de ciberseguridad a nivel de la Unión y apoyará a los Estados miembros y a las instituciones, órganos y organismos de la UE en la organización de ejercicios a petición suya. Los ejercicios anuales a nivel de la Unión incluirán elementos técnicos, operativos y estratégicos y contribuirán a preparar la respuesta cooperativa a nivel de la Unión a los incidentes de ciberseguridad a gran escala y de carácter transfronterizo. La Agencia participará asimismo en la realización de ejercicios sectoriales de ciberseguridad, y contribuirá a organizarlos cuando proceda, junto con los ISAC pertinentes y permitirá a los ISAC participar también en los ejercicios de ciberseguridad a nivel de la Unión.
7. La Agencia elaborará un informe periódico sobre la situación técnica de la ciberseguridad en la UE, relativo a incidentes y amenazas, basándose en la información de fuentes abiertas, en su propio análisis y en los informes comunicados, entre otros, por los CSIRT de los Estados miembros (con carácter voluntario) o los puntos de contacto únicos de la Directiva SRI (de conformidad con su artículo 14, apartado 5), el Centro Europeo de Ciberdelincuencia (EC3) de Europol y el CERT-UE.
8. La Agencia contribuirá a desarrollar una respuesta cooperativa, a nivel de la Unión y de Estado miembro, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad, principalmente por los siguientes medios:
 - a) agregación de los informes procedentes de fuentes nacionales, con vistas a contribuir a la creación de una perspectiva común de la situación;
 - b) garantía de la eficacia del flujo de información y oferta de mecanismos de intensificación entre la red de CSIRT y los responsables políticos y técnicos a nivel de la Unión;
 - c) apoyo a la gestión técnica de un incidente o crisis, en particular facilitando la puesta en común de soluciones técnicas entre los Estados miembros;
 - d) apoyo a la comunicación pública en torno al incidente o crisis;
 - e) ensayo de los planes de cooperación para responder a estos incidentes o crisis.

Artículo 8

Tareas relativas al mercado, certificación de la ciberseguridad y normalización

La Agencia:

- a) Apoyará y promoverá el desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de productos y servicios de TIC, según lo establecido en el título III del presente Reglamento, por los siguientes medios:

- 1) preparar propuestas de regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC de conformidad con el artículo 44 del presente Reglamento;
 - 2) asistir a la Comisión, encargándose de la secretaría del Grupo Europeo de Certificación de la Ciberseguridad de conformidad con el artículo 53 del presente Reglamento;
 - 3) recopilar y publicar directrices y desarrollar buenas prácticas relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la industria.
- b) Facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos y servicios de TIC y elaborará, en colaboración con los Estados miembros, directrices y orientaciones relativas a las áreas técnicas relacionadas con los requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, así como relativas a normas ya existentes, entre ellas las normas nacionales de los Estados miembros, con arreglo al artículo 19, apartado 2, de la Directiva (UE) 2016/1148.
- c) Realizará y difundirá análisis periódicos de las principales tendencias en el mercado de la ciberseguridad, tanto del lado de la oferta como de la demanda, con el fin de fomentar dicho mercado en la Unión.

Artículo 9

Tareas relativas al conocimiento, la información y la sensibilización

La Agencia:

- a) efectuará análisis de las tecnologías emergentes y preparará evaluaciones temáticas sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas sobre la ciberseguridad;
- b) realizará análisis estratégicos a largo plazo de las amenazas e incidentes de ciberseguridad, con el fin de detectar las tendencias emergentes y ayudar a prevenir los problemas relacionados con la ciberseguridad;
- c) aportará, en cooperación con los expertos de las autoridades de los Estados miembros, dictámenes, directrices y mejores prácticas para la seguridad de las redes y los sistemas de información, en particular en el ámbito de la seguridad de la infraestructura de internet y de las infraestructuras que sustentan los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148;
- d) reunirá, organizará y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión;
- e) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas para usuarios individuales, dirigidas a ciudadanos y organizaciones;
- f) recopilará y analizará la información disponible públicamente relativa a incidentes significativos y elaborará informes con el fin de ofrecer orientaciones a las empresas y ciudadanos de toda la Unión;

- g) organizará, en cooperación con los Estados miembros y las instituciones, órganos y organismos de la Unión, campañas periódicas de divulgación para aumentar la ciberseguridad y su visibilidad en la Unión.

Artículo 10

Tareas relativas a la investigación y la innovación

En relación con la investigación y la innovación, la Agencia:

- a) asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo;
- b) participará, cuando la Comisión le haya delegado los poderes correspondientes, en la fase de ejecución de los programas de financiación de la investigación y la innovación, o en calidad de beneficiario.

Artículo 11

Tareas relativas a la cooperación internacional

La Agencia contribuirá a los esfuerzos de la Unión por cooperar con terceros países y organizaciones internacionales a fin de promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad, por los siguientes medios:

- a) participar, cuando proceda, como observador en la organización de ejercicios internacionales, y analizar los resultados de esos ejercicios e informar al respecto al Consejo de Administración;
- b) facilitar, a petición de la Comisión, el intercambio de mejores prácticas entre las organizaciones internacionales pertinentes;
- c) facilitar asesoramiento a la Comisión cuando así se solicite.

CAPÍTULO II ORGANIZACIÓN DE LA AGENCIA

Artículo 12

Estructura

La estructura administrativa y de gestión de la Agencia estará integrada por los siguientes elementos:

- a) un Consejo de Administración, que ejercerá las funciones definidas en el artículo 14;
- b) un Comité Ejecutivo, que ejercerá las funciones definidas en el artículo 18;
- c) un director ejecutivo, con las responsabilidades definidas en el artículo 19; y

- d) un Grupo Permanente de Partes Interesadas, que ejercerá las funciones definidas en el artículo 20.

SECCIÓN 1

CONSEJO DE ADMINISTRACIÓN

Artículo 13

Composición del Consejo de Administración

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y dos representantes nombrados por la Comisión. Todos los representantes tendrán derecho a voto.
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 de la ciberseguridad, teniendo en cuenta las pertinentes cualificaciones presupuestarias, administrativas y de 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 alcanzar una representación equilibrada entre hombres y mujeres en el Consejo de Administración.
4. El mandato de los miembros del Consejo de Administración y de sus suplentes será de cuatro años. Este mandato será renovable.

Artículo 14

Funciones del Consejo de Administración

1. El Consejo de Administración:
 - a) definirá la orientación general del funcionamiento de la Agencia y velará por que esta trabaje de conformidad con las normas y principios establecidos en el presente Reglamento; velará asimismo por la coherencia de la labor de la Agencia con las actividades realizadas por los Estados miembros y a nivel de la Unión;
 - b) adoptará el proyecto de documento único de programación de la Agencia a que se refiere el artículo 21 antes de someterlo al dictamen de la Comisión;
 - c) adoptará, teniendo en cuenta el dictamen de la Comisión, el documento único de programación de la Agencia por una mayoría de dos tercios de sus miembros y de conformidad con el artículo 17;
 - d) adoptará, por mayoría de dos tercios de sus miembros, el presupuesto anual de la Agencia y ejercerá otras funciones relacionadas con el presupuesto de la Agencia con arreglo al capítulo III;
 - e) evaluará y adoptará el informe anual consolidado sobre las actividades de la Agencia y, a más tardar el 1 de julio del año siguiente, remitirá dicho informe, junto con su evaluación, al Parlamento Europeo, al Consejo, a la

Comisión y al Tribunal de Cuentas; el informe anual incluirá las cuentas y describirá en qué medida la Agencia ha cumplido sus indicadores de rendimiento; el informe anual se hará público;

- f) adoptará las normas financieras aplicables a la Agencia de conformidad con el artículo 29;
- g) 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;
- h) adoptará normas para la prevención y la gestión de los conflictos de intereses de sus miembros;
- i) garantizará un adecuado seguimiento de las conclusiones y recomendaciones resultantes de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF) o de las diferentes auditorías y evaluaciones, tanto internas como externas;
- j) adoptará su propio reglamento interno;
- k) de conformidad con el apartado 2, ejercerá, respecto del personal de la Agencia, las competencias atribuidas por el Estatuto de los funcionarios a la Autoridad facultada para proceder a los nombramientos y las atribuidas por el Régimen aplicable a los otros agentes de la Unión Europea a la Autoridad facultada para proceder a las contrataciones (en lo sucesivo, «las competencias de la Autoridad facultada para proceder a los nombramientos»);
- l) adoptará las normas de aplicación del Estatuto de los funcionarios y del Régimen aplicable a los otros agentes, de acuerdo con el procedimiento establecido en el artículo 110 de dicho Estatuto;
- m) nombrará al director ejecutivo y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 33 del presente Reglamento;
- n) nombrará a un contable, que podrá ser el contable de la Comisión, que será totalmente independiente en el desempeño de sus funciones;
- o) adoptará todas las decisiones relativas al establecimiento de las estructuras internas de la Agencia y, cuando sea necesario, a su modificación, teniendo en cuenta las necesidades de la actividad de la Agencia, así como la buena gestión financiera;
- p) autorizará la celebración de convenios de trabajo de conformidad con los artículos 7 y 39.

2. 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 y en el artículo 6 del Régimen aplicable a los otros agentes, por la que se delegarán las competencias de la autoridad facultada para proceder a los nombramientos en el director ejecutivo y se definirán las condiciones en las que podrá suspenderse la delegación de competencias. El director ejecutivo estará autorizado a subdelegar esas competencias.
3. Cuando así lo exijan circunstancias excepcionales, el Consejo de Administración podrá, mediante resolución, suspender temporalmente la delegación de las competencias de la Autoridad facultada para proceder a los nombramientos en el

director ejecutivo y la subdelegación de competencias por parte de este último, y ejercer él mismo las competencias o delegarlas en uno de sus miembros o en un miembro del personal distinto del director ejecutivo.

Artículo 15

Presidente del Consejo de Administración

El Consejo de Administración elegirá entre sus miembros, por mayoría de dos tercios, a un presidente y a un vicepresidente para un período de cuatro años, que será renovable una sola vez. No obstante, si el presidente o el vicepresidente dejaran de ser miembros del Consejo de Administración durante su mandato, este expirará automáticamente en la misma fecha. El vicepresidente sustituirá de oficio al presidente cuando este no pueda desempeñar sus funciones.

Artículo 16

Reuniones del Consejo de Administración

1. Las reuniones del Consejo de Administración serán convocadas por su presidente.
2. El Consejo de Administración se reunirá al menos dos veces al año en sesión ordinaria. Celebrará también sesiones extraordinarias a instancias del presidente, de la Comisión o de como mínimo un tercio de sus miembros.
3. El director ejecutivo asistirá, sin tener derecho a voto, a las reuniones del Consejo de Administración.
4. Los miembros del Grupo Permanente de Partes Interesadas del sector podrán participar, previa invitación del presidente, en las reuniones del Consejo de Administración, sin derecho a voto.
5. Los miembros del Consejo de Administración y sus suplentes podrán estar asistidos en las reuniones por asesores o expertos, con sujeción a su reglamento interno.
6. La Agencia se encargará de la secretaría del Consejo de Administración.

Artículo 17

Votaciones en el Consejo de Administración

1. El Consejo de Administración tomará sus decisiones por mayoría de sus miembros.
2. Se requerirá una mayoría de dos tercios de todos los miembros del Consejo de Administración para aprobar el documento único de programación, el presupuesto anual y el nombramiento, prórroga del mandato o cese del director ejecutivo.
3. Cada miembro dispondrá de un voto. En ausencia de un miembro, su suplente podrá ejercer su derecho a voto.
4. El presidente participará en las votaciones.
5. El director ejecutivo no participará en las votaciones.
6. El reglamento interno del Consejo de Administración establecerá de manera más pormenorizada el régimen de votación, en particular las condiciones en las que un miembro puede actuar por cuenta de otro.

SECCIÓN 2

COMITÉ EJECUTIVO

Artículo 18

Comité Ejecutivo

1. El Consejo de Administración estará asistido por un Comité Ejecutivo.
2. El Comité Ejecutivo:
 - a) preparará las resoluciones que deba adoptar el Consejo de Administración;
 - b) junto con el Consejo de Administración, garantizará un seguimiento adecuado de las conclusiones y recomendaciones que se deriven de las investigaciones de la OLAF y de las distintas auditorías y evaluaciones tanto internas como externas;
 - c) sin perjuicio de las responsabilidades del director ejecutivo establecidas en el artículo 19, le asistirá y asesorará en la aplicación de las decisiones del Consejo de Administración en cuestiones administrativas y presupuestarias con arreglo al artículo 19.
3. El Comité Ejecutivo estará formado por cinco miembros escogidos entre los miembros del Consejo de Administración, entre los que figurarán el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y uno de los representantes de la Comisión. El director ejecutivo participará en las reuniones del Comité Ejecutivo, pero no tendrá derecho de voto.
4. La duración del mandato de los miembros del Comité Ejecutivo será de cuatro años. Este mandato será renovable.
5. El Comité Ejecutivo se reunirá al menos una vez cada tres meses. El presidente del Comité Ejecutivo convocará otras reuniones a petición de sus miembros.
6. El Consejo de Administración establecerá el reglamento interno del Comité Ejecutivo.
7. Cuando sea necesario, por motivos de urgencia, el Comité Ejecutivo podrá adoptar determinadas decisiones provisionales en nombre del Consejo de Administración, en particular en materia de gestión administrativa, incluida la suspensión de la delegación de las competencias atribuidas a la autoridad facultada para proceder a los nombramientos, y para cuestiones presupuestarias.

SECCIÓN 3

DIRECTOR EJECUTIVO

Artículo 19

Responsabilidades del director ejecutivo

1. La Agencia será gestionada por su director ejecutivo, que deberá actuar con independencia en el desempeño de sus funciones. El director ejecutivo dará cuenta de su gestión al Consejo de Administración.

2. El director ejecutivo informará al Parlamento Europeo sobre el ejercicio de sus funciones cuando se le invite a hacerlo. El Consejo podrá convocar al director ejecutivo para que le informe sobre el ejercicio de sus funciones.
3. El director ejecutivo será responsable de:
 - a) la administración ordinaria de la Agencia;
 - b) ejecutar las decisiones adoptadas por el Consejo de Administración;
 - c) preparar el proyecto de documento único de programación y presentarlo al Consejo de Administración para su aprobación antes de su presentación a la Comisión;
 - d) ejecutar el documento único de programación y presentar informes al respecto al Consejo de Administración;
 - e) preparar el informe anual consolidado sobre las actividades de la Agencia y presentarlo al Consejo de Administración para su evaluación y aprobación;
 - f) preparar un plan de acción para el seguimiento de las conclusiones de las evaluaciones retrospectivas e informar cada dos años a la Comisión sobre los progresos al respecto;
 - g) preparar un plan de acción sobre la base de las conclusiones 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 conseguidos, dos veces al año a la Comisión y regularmente al Consejo de Administración;
 - h) preparar el proyecto de normas financieras aplicables a la Agencia;
 - i) preparar el proyecto de estado de previsiones de ingresos y gastos de la Agencia y ejecutar su presupuesto;
 - j) proteger 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;
 - k) preparar una estrategia antifraude para la Agencia y someterla a la aprobación del Consejo de Administración;
 - l) crear y mantener contactos con la comunidad empresarial y las organizaciones de consumidores para garantizar un diálogo continuado con las partes interesadas pertinentes;
 - m) desempeñar otros cometidos que el presente Reglamento le asigne.
4. Siempre que sea necesario y esté dentro del mandato de la Agencia, y de conformidad con sus objetivos y tareas, el director ejecutivo podrá crear grupos de trabajo *ad hoc* integrados por expertos, incluidos expertos procedentes de las autoridades competentes de los Estados miembros. Se informará de ello anticipadamente al Consejo de Administración. Los procedimientos, en particular en

lo que se refiere a la composición de los grupos de trabajo, el nombramiento de los expertos de dichos grupos por el director ejecutivo y el funcionamiento de los grupos de trabajo, se especificarán en el reglamento operativo interno de la Agencia.

5. El director ejecutivo decidirá si es necesario ubicar a miembros de su personal en uno o más Estados miembros con el fin de desempeñar las funciones de la Agencia de manera eficiente y eficaz. Antes de tomar la decisión de establecer una oficina local, el director ejecutivo habrá de obtener el consentimiento previo de la Comisión, el Consejo de Administración y el Estado o Estados miembros de que se trate. Esta decisión especificará el alcance de las actividades que se llevarán a cabo en la oficina local, evitándose costes innecesarios y la duplicación de funciones administrativas de la Agencia. Se llegará a un acuerdo con el Estado o Estados miembros de que se trate, cuando resulte apropiado o necesario.

SECCIÓN 4

GRUPO PERMANENTE DE PARTES INTERESADAS

Artículo 20

Grupo Permanente de Partes Interesadas

1. El Consejo de Administración establecerá, a propuesta del director ejecutivo, un Grupo Permanente de Partes Interesadas integrado por expertos reconocidos que representen a las partes interesadas pertinentes, tales como la industria de las TIC, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, los grupos de consumidores, expertos académicos en ciberseguridad y representantes de las autoridades competentes notificadas con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas] y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos.
2. Los procedimientos del Grupo Permanente de Partes Interesadas, en particular con respecto al número, composición y nombramiento de sus miembros por el Consejo de Administración, a la propuesta por el director ejecutivo y al funcionamiento del Grupo, se especificarán en el reglamento operativo interno de la Agencia y se harán públicos.
3. El Grupo Permanente de Partes Interesadas estará presidido por el director ejecutivo o cualquier otra persona que este designe en cada caso.
4. El mandato de los miembros del Grupo Permanente de Partes Interesadas tendrá una duración de dos años y medio. Los miembros del Consejo de Administración no podrán ser miembros del Grupo Permanente de Partes Interesadas. Los expertos de la Comisión y de los Estados miembros podrán estar presentes en las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos. Se podrá invitar a asistir a las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos a representantes de otros órganos que no sean miembros del mismo y el director ejecutivo considere pertinentes.
5. El Grupo Permanente de Partes Interesadas asesorará a la Agencia en lo relativo a la realización de sus actividades. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo de la Agencia y en el

mantenimiento de la comunicación con las partes interesadas pertinentes sobre todos los aspectos relativos al programa de trabajo.

SECCIÓN 5

FUNCIONAMIENTO

Artículo 21

Documento único de programación

1. La Agencia llevará a cabo sus operaciones de conformidad con un documento único de programación que contendrá su programación anual y plurianual, con inclusión de la totalidad de sus actividades previstas.
2. Cada año, el director ejecutivo elaborará un proyecto de documento único de programación que contendrá la programación anual y plurianual, con la planificación de los recursos humanos y financieros correspondientes, de conformidad con el artículo 32 del Reglamento Delegado (UE) n.º 1271/2013 de la Comisión³⁶ y teniendo en cuenta las directrices establecidas por la Comisión.
3. A más tardar el 30 de noviembre de cada año, el Consejo de Administración adoptará el documento único de programación a que se refiere el apartado 1 y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión a más tardar el 31 de enero del año siguiente, así como cualquier versión posterior actualizada de dicho documento.
4. El documento único de programación será definitivo tras la adopción final del presupuesto general de la Unión y, en caso necesario, se adaptará en consecuencia.
5. El programa de trabajo anual incluirá objetivos detallados y los resultados esperados, incluidos indicadores de rendimiento. Contendrá asimismo una descripción de las acciones que vayan a financiarse y una indicación de los recursos humanos y financieros asignados a cada acción, de conformidad con los principios de presupuestación y gestión por actividades. El programa anual de trabajo será coherente con el programa de trabajo plurianual a que se refiere el apartado 7. Indicará claramente qué tareas se han añadido, modificado o suprimido en relación con el ejercicio presupuestario anterior.
6. El Consejo de Administración modificará el programa de trabajo anual adoptado cuando se encomiende una nueva tarea a la Agencia. Cualquier modificación sustancial del programa de trabajo anual se adoptará con arreglo al mismo procedimiento que el programa de trabajo anual inicial. El Consejo de Administración podrá delegar en el director ejecutivo la facultad de adoptar modificaciones no sustanciales del programa de trabajo anual.
7. El programa de trabajo plurianual fijará la programación estratégica general, incluidos los objetivos, los resultados esperados y los indicadores de rendimiento.

³⁶ 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).

Definirá asimismo la programación de los recursos, incluidos el presupuesto plurianual y el personal.

8. La programación de los recursos se actualizará todos los años. La programación estratégica se actualizará cuando proceda, y en particular cuando resulte necesario a la luz de los resultados de la evaluación a que se refiere el artículo 56.

Artículo 22

Declaración de intereses

1. Los miembros del Consejo de Administración, el director ejecutivo y los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal deberán efectuar cada uno de ellos una declaración de compromisos y otra declaración en la que indiquen si tienen o no intereses directos o indirectos que pudieran considerarse perjudiciales para su independencia. Las declaraciones serán exactas y completas, se presentarán anualmente por escrito y se actualizarán siempre que sea necesario.
2. Los miembros del Consejo de Administración, el director ejecutivo y los expertos externos que participen en los grupos de trabajo *ad hoc* deberán declarar cada uno de ellos de forma exacta y completa, a más tardar al comienzo de cada reunión, cualquier interés que pudiera considerarse perjudicial para su independencia en relación con los puntos del orden del día y deberán abstenerse de participar en los debates y en la votación sobre esos puntos.
3. La Agencia establecerá en su reglamento operativo interno las medidas prácticas correspondientes a las normas sobre declaraciones de intereses a que se refieren los apartados 1 y 2.

Artículo 23

Transparencia

1. La Agencia llevará a cabo sus actividades con un alto grado de transparencia y de conformidad con el artículo 25.
2. La Agencia velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 22.
3. El Consejo de Administración, a propuesta del director ejecutivo, podrá autorizar a otras partes interesadas a participar en calidad de observadores en algunas de las actividades de la Agencia.
4. La Agencia establecerá en su reglamento operativo interno las medidas prácticas de aplicación de las normas de transparencia a que se refieren los apartados 1 y 2.

Artículo 24

Confidencialidad

1. Sin perjuicio de lo dispuesto en el artículo 25, la Agencia no divulgará a terceros la información que procese o reciba para la que se haya presentado una solicitud motivada de tratamiento confidencial referida a todo la información o a parte de ella.

2. Los miembros del Consejo de Administración, el director ejecutivo, los miembros del Grupo Permanente de Partes Interesadas, los expertos externos que participen en los grupos de trabajo *ad hoc* y los miembros del personal de la Agencia, incluidos los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal, respetarán la obligación de confidencialidad en virtud del artículo 339 del Tratado de Funcionamiento de la Unión Europea (TFUE), incluso después de haber cesado en sus cargos.
3. La Agencia establecerá en su reglamento operativo interno las medidas prácticas de aplicación de las normas de confidencialidad a que se refieren los apartados 1 y 2.
4. Si así lo exige el desempeño de los cometidos de la Agencia, el Consejo de Administración tomará la decisión de permitir a la Agencia manejar información clasificada. En tal caso, el Consejo de Administración, de común acuerdo con los servicios de la Comisión, adoptará un reglamento operativo interno que aplique los principios de seguridad contenidos en las Decisiones (UE, Euratom) 2015/443³⁷ y 2015/444³⁸ de la Comisión. Dicho reglamento incluirá, entre otras, disposiciones para el intercambio, tratamiento y almacenamiento de la información clasificada.

Artículo 25

Acceso a los documentos

1. Se aplicará a los documentos en poder de la Agencia el Reglamento (CE) n.º 1049/2001.
2. El Consejo de Administración adoptará disposiciones para la aplicación del Reglamento (CE) n.º 1049/2001 en el plazo de seis meses a partir del establecimiento de la Agencia.
3. Las decisiones tomadas por la Agencia en virtud del 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 TFUE o de un recurso ante el Tribunal de Justicia de la Unión Europea de conformidad con el artículo 263 del TFUE.

CAPÍTULO III

ESTABLECIMIENTO Y ESTRUCTURA DEL PRESUPUESTO

Artículo 26

Establecimiento del presupuesto

1. El director ejecutivo elaborará cada año un proyecto de declaración sobre la previsión de los ingresos y los gastos de la Agencia para el siguiente ejercicio financiero, y lo hará llegar al Consejo de Administración, junto con un proyecto de plantilla. Los ingresos y los gastos deberán estar equilibrados.

³⁷ [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).

³⁸ [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).

2. El Consejo de Administración presentará cada año, sobre la base del proyecto de previsión de ingresos y gastos a que se refiere el apartado 1, la previsión de ingresos y gastos de la Agencia para el siguiente ejercicio financiero.
3. El Consejo de Administración, a más tardar el 31 de enero de cada año, transmitirá la previsión a que se refiere el apartado 2, que formará parte del proyecto de documento único de programación, a la Comisión y a los terceros países con los que la Unión haya celebrado acuerdos de conformidad con el artículo 39.
4. Sobre la base de dicha previsión, la Comisión consignará en el proyecto de presupuesto general de la Unión Europea 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 a la Agencia.
6. El Parlamento Europeo y el Consejo aprobarán la plantilla de la Agencia.
7. Junto con el documento único de programación, el Consejo de Administración adoptará el presupuesto de la Agencia. Este se convertirá en definitivo tras la adopción final del presupuesto general de la Unión Europea. Cuando proceda, el Consejo de Administración reajustará el presupuesto y el documento único de programación de la Agencia con arreglo al presupuesto general de la Unión Europea.

Artículo 27

Estructura del presupuesto

1. Sin perjuicio de otros recursos, los ingresos de la Agencia consistirán en:
 - a) una contribución procedente del presupuesto de la Unión;
 - b) ingresos asignados a partidas de gastos específicas de conformidad con sus normas financieras mencionadas en el artículo 29;
 - c) financiación de la Unión en forma de convenios de delegación o subvenciones *ad hoc*, de conformidad con sus normas financieras mencionadas en el artículo 29 y las disposiciones de los instrumentos pertinentes de apoyo a las políticas de la Unión;
 - d) contribuciones de terceros países que participen en los trabajos de la Agencia tal como prevé el artículo 39;
 - e) eventuales contribuciones voluntarias de los Estados miembros en efectivo o en especie; los Estados miembros que aporten contribuciones voluntarias no podrán reclamar ningún derecho o servicio específico como consecuencia de su contribución.
2. Los gastos de la Agencia incluirán los gastos de personal, administrativos y de soporte técnico, de infraestructura y funcionamiento, así como los gastos derivados de contratos suscritos con terceros.

Artículo 28
Ejecución del presupuesto

1. El director ejecutivo será responsable de la ejecución del presupuesto de la Agencia.
2. El auditor interno de la Comisión ejercerá, con respecto a la Agencia, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión.
3. A más tardar el 1 de marzo siguiente a un ejercicio financiero (1 de marzo del año N+1), el contable de la Agencia remitirá las cuentas provisionales al contable de la Comisión y al Tribunal de Cuentas.
4. Tras recibir las observaciones formuladas por el Tribunal de Cuentas sobre las cuentas provisionales de la Agencia, el contable de esta elaborará las cuentas definitivas de la Agencia bajo su responsabilidad.
5. El director ejecutivo presentará las cuentas definitivas al Consejo de Administración para que este emita dictamen al respecto.
6. A más tardar el 31 de marzo del año N + 1, el director ejecutivo remitirá el informe sobre la gestión presupuestaria y financiera al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas.
7. A más tardar el 1 de julio del año N + 1, el contable remitirá las cuentas definitivas, juntamente con el dictamen del Consejo de Administración, al Parlamento Europeo, al Consejo, al contable de la Comisión y al Tribunal de Cuentas.
8. En la misma fecha de transmisión de sus cuentas definitivas, el contable también enviará al Tribunal de Cuentas una toma de posición relativa a estas cuentas definitivas, con copia al contable de la Comisión.
9. El director ejecutivo publicará las cuentas definitivas a más tardar el 15 de noviembre del año siguiente.
10. El director ejecutivo remitirá al Tribunal de Cuentas una respuesta a sus observaciones a más tardar el 30 de septiembre del año N + 1, y enviará asimismo copia de dicha respuesta al Consejo de Administración y a la Comisión.
11. El director ejecutivo presentará al Parlamento Europeo, cuando este lo solicite, toda la información necesaria para el correcto desarrollo del procedimiento de aprobación de la ejecución del presupuesto del ejercicio de que se trate, según se establece en el artículo 165, apartado 3, del Reglamento Financiero.
12. El Parlamento Europeo, sobre la base de una recomendación del Consejo, deberá aprobar la gestión del director ejecutivo antes del 15 de mayo del año N + 2 respecto a la ejecución del presupuesto del año N.

Artículo 29
Normas financieras

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

Artículo 30
Lucha contra el fraude

1. Con el fin de facilitar la lucha contra el fraude, la corrupción y otras actividades ilegales con arreglo al Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo³⁹, la Agencia, en el plazo de seis meses a partir de la fecha en que comience a operar, suscribirá el Acuerdo Interinstitucional, de 25 de mayo de 1999, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF), y adoptará las disposiciones pertinentes, que serán de aplicación a todo el personal de la Agencia, sirviéndose del modelo contenido en el anexo de dicho Acuerdo.
2. El Tribunal de Cuentas tendrá la facultad de auditar, sobre la base de documentos y sobre el terreno, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido de la Agencia fondos de la Unión.
3. La OLAF podrá realizar investigaciones, incluidos controles y verificaciones sobre el terreno, de conformidad con las disposiciones y los procedimientos establecidos en el Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo y el Reglamento (Euratom, CE) n.º 2185/96 del Consejo⁴⁰, 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, 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 la Agencia.
4. Sin perjuicio de lo dispuesto en los apartados 1, 2 y 3, los acuerdos de cooperación con terceros países y con organizaciones internacionales, así como los contratos y los convenios y decisiones de subvención de la Agencia, contendrán disposiciones que establezcan expresamente la potestad del Tribunal de Cuentas y de la OLAF de llevar a cabo las auditorías y las investigaciones mencionadas, según sus respectivas competencias.

CAPÍTULO IV
PERSONAL DE LA AGENCIA

Artículo 31
Disposiciones generales

Se aplicarán al personal de la Agencia el Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, así como las normas adoptadas por acuerdo entre las instituciones de la Unión con el fin de poner en práctica tales disposiciones.

³⁹ [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).

⁴⁰ [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).

Artículo 32
Privilegios e inmunidades

Se aplicará a la Agencia y a su personal el Protocolo n.º 7 sobre los privilegios y las inmunidades de la Unión Europea, anejo al Tratado de la Unión Europea y al TFUE.

Artículo 33
Director ejecutivo

1. El director ejecutivo será contratado como agente temporal de la Agencia según lo dispuesto en el artículo 2, letra a), del Régimen aplicable a los otros agentes.
2. El director ejecutivo será nombrado por el Consejo de Administración a partir de una lista de candidatos propuesta por la Comisión en el marco de un procedimiento de selección abierto y transparente.
3. Para la celebración del contrato del director ejecutivo, la Agencia estará representada por el presidente del Consejo de Administración.
4. Antes del nombramiento, se invitará al candidato seleccionado por el Consejo de Administración a hacer una declaración ante la comisión pertinente del Parlamento Europeo y a responder a las preguntas formuladas por los parlamentarios.
5. El mandato del director ejecutivo tendrá una duración de cinco años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las futuras tareas y desafíos de la Agencia.
6. El Consejo de Administración se pronunciará sobre el nombramiento, la prórroga del mandato o el cese del director ejecutivo por mayoría de dos tercios de sus miembros con derecho de voto.
7. A propuesta de la Comisión, en la que se tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá prorrogar una vez el mandato del director ejecutivo, por un plazo máximo de cinco años.
8. El Consejo de Administración informará al Parlamento Europeo acerca de su intención de prorrogar el mandato del director ejecutivo. En los tres meses que precedan a la prórroga de su mandato, el director ejecutivo hará, si se le invita a ello, una declaración ante la comisión pertinente del Parlamento Europeo y responderá a las preguntas formuladas por los parlamentarios.
9. Un director ejecutivo cuyo mandato haya sido prorrogado no podrá participar en otro procedimiento de selección para el mismo puesto.
10. El director ejecutivo solo podrá ser cesado por una decisión del Consejo de Administración, a propuesta de la Comisión.

Artículo 34
Expertos nacionales en comisión de servicios y otros agentes

1. La Agencia podrá recurrir a expertos nacionales en comisión de servicios o a otro personal no contratado por la Agencia. El Estatuto de los funcionarios y el Régimen aplicable a los otros agentes no serán de aplicación a este personal.
2. El Consejo de Administración adoptará una decisión que establezca las normas aplicables a las comisiones de servicios de expertos nacionales en la Agencia.

CAPÍTULO V

DISPOSICIONES GENERALES

Artículo 35

Estatuto jurídico de la Agencia

1. La Agencia será un órgano de la Unión dotado de personalidad jurídica.
2. En cada Estado miembro, la Agencia disfrutará de la capacidad jurídica más amplia que se conceda a las personas jurídicas en el Derecho interno. En particular, podrá adquirir o vender propiedad mobiliaria e inmobiliaria y ser parte en actuaciones judiciales.
3. La Agencia estará representada por su director ejecutivo.

Artículo 36

Responsabilidad de la Agencia

1. La responsabilidad contractual de la Agencia se regirá por la legislación aplicable al contrato de que se trate.
2. El Tribunal de Justicia de la Unión Europea será competente para pronunciarse en virtud de cualquier cláusula arbitral contenida en un contrato firmado por la Agencia.
3. En materia de responsabilidad extracontractual, la Agencia deberá reparar los daños causados por ella o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a las legislaciones de los Estados miembros.
4. El Tribunal de Justicia de la Unión Europea será competente para conocer de todos los litigios relativos a la indemnización por esos daños.
5. La responsabilidad personal de los agentes respecto a la Agencia se regirá por las disposiciones pertinentes aplicables al personal de la Agencia.

Artículo 37

Régimen lingüístico

1. Se aplicarán a la Agencia las disposiciones establecidas en el Reglamento n.º 1⁴¹. Los Estados miembros y los demás organismos nombrados por ellos podrán dirigirse a la Agencia y obtener respuesta en la lengua oficial de las instituciones de la Unión Europea que elijan.
2. Los servicios de traducción requeridos para el funcionamiento de la Agencia serán prestados por el Centro de Traducción de los Órganos de la Unión Europea.

⁴¹

[Reglamento n.º 1 por el que se fija el régimen lingüístico de la Comunidad Europea de la Energía Atómica](#) (DO 17 de 6.10.1958, p. 401).

Artículo 38

Protección de los datos personales

1. El tratamiento de los datos personales por parte de la Agencia deberá ajustarse al Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo⁴².
2. El Consejo de Administración adoptará las normas complementarias a que se refiere el artículo 24, apartado 8, del Reglamento (CE) n.º 45/2001. El Consejo de Administración podrá adoptar otras medidas necesarias para la aplicación del Reglamento (CE) n.º 45/2001 por parte de la Agencia.

Artículo 39

Cooperación con terceros países y organizaciones internacionales

1. En la medida en que resulte necesario para el logro de los objetivos fijados en el presente Reglamento, la Agencia podrá cooperar con las autoridades competentes de terceros países, con organizaciones internacionales, o con ambas. Para ello, la Agencia podrá, previa aprobación de la Comisión, establecer acuerdos de trabajo con las autoridades de terceros países y organizaciones internacionales. Dichos acuerdos no impondrán obligaciones jurídicas que incumban a la Unión y sus Estados miembros.
2. La Agencia estará abierta a la participación de terceros países que hayan celebrado acuerdos con la Unión en este sentido. Con arreglo a las disposiciones pertinentes de dichos acuerdos, se irán estableciendo mecanismos que precisen, en particular, el carácter, el alcance y las modalidades de participación de cada uno de estos países en la labor de la Agencia, incluidas disposiciones sobre la participación en las iniciativas emprendidas por la Agencia, las contribuciones financieras y el personal. Por lo que se refiere al personal, dichos mecanismos serán, en cualquier caso, conformes con el Estatuto de los funcionarios.
3. El Consejo de Administración adoptará una estrategia para las relaciones con terceros países u organizaciones internacionales en asuntos en los que sea competente la Agencia. La Comisión velará por que la Agencia opere dentro de su mandato y del marco institucional existente mediante la celebración de un convenio de trabajo adecuado con el director ejecutivo de la Agencia.

Artículo 40

Normas de seguridad aplicables a la protección de la información clasificada y de la información sensible no clasificada

La Agencia, en consulta con la Comisión, adoptará sus normas de seguridad aplicando los principios de seguridad contenidos en las normas de seguridad de la Comisión para la protección de la información clasificada de la Unión Europea (ICUE) y la información sensible no clasificada, según lo dispuesto en las Decisiones (UE, Euratom) 2015/443 y 2015/444. Esto incluirá, entre otras cosas, disposiciones para el intercambio, tratamiento y almacenamiento de este tipo de información.

⁴²

Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

Artículo 41

Acuerdo relativo a la sede y condiciones de funcionamiento

1. Las disposiciones necesarias relativas a la instalación que se habilitará para la Agencia en el Estado miembro de acogida y los recursos que debe poner a su disposición dicho Estado miembro, así como las normas específicas aplicables en el Estado miembro de acogida al director ejecutivo, a los miembros del Consejo de Administración, al personal de la Agencia y a los miembros de sus familias se fijarán en un acuerdo de sede celebrado entre la Agencia y el Estado miembro de acogida concluido, previa aprobación del Consejo de Administración, a más tardar [dos años después de la entrada en vigor del presente Reglamento].
2. El Estado miembro que acoja a la Agencia ofrecerá las mejores condiciones posibles para garantizar su buen funcionamiento, incluida la accesibilidad de su ubicación, la presencia de servicios educativos adecuados para los hijos de los miembros del personal y un acceso adecuado al mercado de trabajo, la seguridad social y la atención médica para hijos y cónyuges.

Artículo 42

Control administrativo

El funcionamiento de la Agencia será supervisado por el Defensor del Pueblo Europeo de conformidad con el artículo 228 del TFUE.

TÍTULO III

MARCO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD

Artículo 43

Regímenes europeos de certificación de la ciberseguridad

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

Artículo 44

Preparación y adopción de un régimen europeo de certificación de la ciberseguridad

1. Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de certificación de la ciberseguridad que cumpla los requisitos expuestos en los artículos 45, 46 y 47 del presente Reglamento. Los Estados miembros o el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») establecido de conformidad con el artículo 53 podrán proponer a la Comisión la preparación de un régimen europeo de certificación de la ciberseguridad.
2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ENISA consultará a todas las partes interesadas y cooperará estrechamente con el Grupo. El Grupo facilitará a ENISA la asistencia y el asesoramiento experto que requiera en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes en caso necesario.
3. ENISA transmitirá a la Comisión la propuesta de régimen europeo de certificación de la ciberseguridad preparada de conformidad con el apartado 2 del presente artículo.
4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento.
5. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los regímenes europeos de certificación de la ciberseguridad y darles publicidad.

Artículo 45

Objetivos de seguridad de los regímenes europeos de certificación de la ciberseguridad

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

- a) proteger los datos almacenados, transmitidos o procesados de otro modo frente al almacenamiento, procesamiento, acceso o revelación accidentales o no autorizados;
- b) proteger los datos almacenados, transmitidos o procesados de otro modo frente a la destrucción accidental o no autorizada, la pérdida accidental o la alteración;
- c) garantizar que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso;
- d) registrar qué datos, funciones o servicios se han comunicado, en qué momentos y por quién;
- e) garantizar que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso o de uso, en qué momentos y por quién;
- f) restaurar la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico;
- g) garantizar que los productos y servicios de TIC se entreguen siempre con un *software* actualizado, que no contenga vulnerabilidades conocidas, y dispongan de mecanismos para efectuar actualizaciones de seguridad del *software*.

Artículo 46

Niveles de garantía de los regímenes europeos de certificación de la ciberseguridad

1. Un régimen europeo de certificación de la ciberseguridad podrá especificar uno o más de los siguientes niveles de garantía: básico, sustancial y/o elevado, para los productos y servicios de TIC amparados en dicho régimen.
2. Los niveles de garantía básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente:
 - a) el nivel de garantía bajo se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado limitado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;
 - b) el nivel de garantía sustancial se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado sustancial de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir sustancialmente el riesgo de incidentes de ciberseguridad;
 - c) el nivel de garantía elevado se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC superior al de los certificados con nivel de garantía sustancial, y se caracteriza en referencia a especificaciones

técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.

Artículo 47

Elementos de los regímenes europeos de certificación de la ciberseguridad

1. Un régimen europeo de certificación de la ciberseguridad incluirá los siguientes elementos:
 - a) objeto y alcance de la certificación, incluido el tipo o categoría de productos y servicios de TIC cubiertos;
 - b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o de la Unión;
 - c) en su caso, uno o varios niveles de garantía;
 - d) criterios y métodos específicos de evaluación, incluidos los tipos de evaluación, para demostrar el logro de los objetivos específicos a que se refiere el artículo 45;
 - e) información necesaria para la certificación que deben facilitar los solicitantes a los organismos de evaluación de la conformidad;
 - f) cuando el régimen prevea marcas o etiquetas, las condiciones en las que pueden utilizarse tales marcas o etiquetas;
 - g) cuando la vigilancia forme parte del régimen, las normas para controlar el cumplimiento de los requisitos de los certificados, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;
 - h) condiciones para la concesión, el mantenimiento, la continuación, la ampliación y la reducción del alcance de la certificación;
 - i) normas relativas a las consecuencias de la no conformidad de los productos y servicios de TIC certificados con los requisitos de certificación;
 - j) normas sobre cómo deben notificarse y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos y servicios de TIC;
 - k) normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad;
 - l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC;
 - m) contenido del certificado expedido.
2. Los requisitos del régimen especificados no podrán contravenir ningún requisito legal aplicable, en particular los que emanen de la legislación armonizada de la Unión.
3. Cuando un acto específico de la Unión así lo prevea, podrá utilizarse la certificación en virtud de un régimen europeo de certificación de la ciberseguridad para demostrar la presunción de conformidad con los requisitos de dicho acto.

4. En ausencia de legislación armonizada de la Unión, la legislación de los Estados miembros podrá prever también el uso de un régimen europeo de certificación de la ciberseguridad para establecer la presunción de conformidad con los requisitos legales.

Artículo 48

Certificación de la ciberseguridad

1. Los productos y servicios de TIC que hayan sido certificados de conformidad con un régimen europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 44 se presumirán conformes con los requisitos de dicho régimen.
2. La certificación será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión.
3. Los organismos de evaluación de la conformidad a que se refiere el artículo 51 expedirán un certificado europeo de ciberseguridad en virtud del presente artículo sobre la base de los criterios incluidos en el régimen europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 44.
4. No obstante lo dispuesto en el apartado 3, en casos debidamente justificados un régimen europeo de ciberseguridad particular podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese régimen. Este organismo público será uno de los siguientes:
 - a) una autoridad nacional de supervisión de la certificación con arreglo al artículo 50, apartado 1;
 - b) un organismo que esté acreditado como organismo de evaluación de la conformidad con arreglo al artículo 51, apartado 1; o
 - c) un organismo establecido con arreglo a las leyes, instrumentos jurídicos u otros procedimientos administrativos oficiales del Estado miembro de que se trate y que cumple los requisitos para los organismos que certifican productos, procesos y servicios con arreglo a la norma ISO/IEC 17065:2012.
5. La persona física o jurídica que presenta sus productos o servicios de TIC al mecanismo de certificación facilitará al organismo de evaluación de la conformidad a que se refiere el artículo 51 toda la información necesaria para llevar a cabo el procedimiento de certificación.
6. Los certificados se expedirán por un período máximo de tres años y podrán renovarse en las mismas condiciones, siempre y cuando sigan cumpliéndose los requisitos correspondientes.
7. Los certificados europeos de ciberseguridad expedidos de conformidad con el presente artículo serán reconocidos en todos los Estados miembros.

Artículo 49

Regímenes y certificados nacionales de certificación de la ciberseguridad

1. Sin perjuicio de lo dispuesto en el apartado 3, los regímenes nacionales de certificación de ciberseguridad y los procedimientos correspondientes para los productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad dejarán de surtir efectos a partir de la fecha establecida en el acto de

ejecución adoptado con arreglo al artículo 44, apartado 4. Los regímenes nacionales de certificación de la ciberseguridad existentes y los procedimientos conexos para los productos y servicios de TIC no cubiertos por un régimen europeo de certificación de la ciberseguridad seguirán existiendo.

2. Los Estados miembros se abstendrán de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad en vigor.
3. Los certificados existentes expedidos de conformidad con regímenes nacionales de certificación de ciberseguridad seguirán siendo válidos hasta su fecha de caducidad.

Artículo 50

Autoridades nacionales de supervisión de la certificación

1. Cada Estado miembro designará una autoridad nacional de supervisión de la certificación.
2. Cada Estado miembro informará a la Comisión de la identidad de la autoridad designada.
3. Las autoridades nacionales de supervisión de la certificación serán, en lo relativo a su organización, sus decisiones de financiación, su estructura jurídica y su proceso de toma de decisiones, independientes de las entidades que están bajo su supervisión.
4. Los Estados miembros velarán por que las autoridades nacionales de supervisión de la certificación dispongan de los recursos adecuados para ejercer sus competencias y llevar a cabo, de manera eficaz y eficiente, las tareas que tienen encomendadas.
5. Para la aplicación eficaz del Reglamento, es conveniente que estas autoridades participen en el Grupo Europeo de Certificación de la Ciberseguridad establecido con arreglo al artículo 53 de manera activa, eficaz, eficiente y segura.
6. Las autoridades nacionales de supervisión de la certificación:
 - a) controlarán e impondrán la aplicación de las disposiciones del presente título a nivel nacional y supervisarán la conformidad de los certificados que hayan sido emitidos por los organismos de evaluación de la conformidad establecidos en sus territorios respectivos con los requisitos establecidos en el presente título y en el correspondiente régimen europeo de certificación de la ciberseguridad;
 - b) controlarán y supervisarán las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento, en particular en relación con la notificación de los organismos de evaluación de la conformidad y las tareas conexas establecidas en el artículo 52 del presente Reglamento;
 - c) tramitarán las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigarán el asunto objeto de la reclamación en la medida que proceda e informarán al reclamante sobre el curso y el resultado de la investigación en un plazo razonable;
 - d) cooperarán con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los

- requisitos del presente Reglamento o de regímenes europeos de ciberseguridad específicos;
- e) seguirán las novedades de interés en el ámbito de la certificación de la ciberseguridad.
7. Cada autoridad nacional de supervisión de la certificación tendrá, como mínimo, las siguientes competencias:
- a) solicitar a los organismos de evaluación de la conformidad y a los titulares de certificados europeos de ciberseguridad que faciliten cualquier información que requiera para el desempeño de sus cometidos;
 - b) llevar a cabo investigaciones, en forma de auditorías, de los organismos de evaluación de la conformidad y los titulares de certificados europeos de ciberseguridad, a efectos de verificar el cumplimiento de lo dispuesto en el título III;
 - c) adoptar las medidas adecuadas, de conformidad con el Derecho nacional, con el fin de garantizar que los organismos de evaluación de la conformidad o los titulares de certificados se ajustan al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad;
 - d) obtener acceso a todos los locales de los organismos de evaluación de la conformidad y los titulares de certificados europeos de ciberseguridad para la realización de investigaciones con arreglo al Derecho de la Unión o al Derecho procesal del Estado miembro;
 - e) retirar, con arreglo al Derecho nacional, los certificados que no se ajusten al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad;
 - f) imponer sanciones, según lo previsto en el artículo 54, con arreglo al Derecho nacional, y solicitar el cese inmediato de la violación de las obligaciones establecidas en el presente Reglamento.
8. Las autoridades nacionales de supervisión de la certificación cooperarán entre ellas y con la Comisión y, en particular, intercambiarán información, experiencias y buenas prácticas en relación con la certificación de la ciberseguridad y las cuestiones técnicas relativas a la ciberseguridad de los productos y servicios de TIC.

Artículo 51

Organismos de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad estarán acreditados por el organismo nacional de acreditación designado con arreglo al Reglamento (CE) n.º 765/2008 solamente si cumplen los requisitos establecidos en el anexo del presente Reglamento.
2. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos establecidos en el presente artículo. Los organismos de acreditación revocarán la acreditación de un organismo de evaluación de la conformidad concedida en virtud del apartado 1 del presente artículo cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la

actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

Artículo 52

Notificación

1. En relación con cada régimen europeo de certificación de la ciberseguridad adoptado con arreglo al artículo 44, las autoridades nacionales de supervisión de la certificación notificarán a la Comisión los correspondientes organismos de evaluación de la conformidad acreditados para expedir certificados de los niveles de garantía especificados en el artículo 46 y, sin dilaciones indebidas, cualquier modificación al respecto.
2. Un año después de la entrada en vigor de un régimen europeo de certificación de la ciberseguridad, la Comisión publicará en el Diario Oficial una lista de los organismos de evaluación de la conformidad notificados.
3. Si la Comisión recibe una notificación una vez concluido el período a que se refiere el apartado 2, publicará en el Diario Oficial de la Unión Europea las modificaciones de la lista a que se refiere el apartado 2 en el plazo de dos meses a partir de la fecha de recepción de dicha notificación.
4. Una autoridad nacional de supervisión de la certificación podrá presentar a la Comisión una solicitud para retirar de la lista a la que se refiere el apartado 2 del presente artículo a un organismo de evaluación de la conformidad notificado por dicha autoridad nacional de supervisión de la certificación. La Comisión publicará en el Diario Oficial de la Unión Europea las modificaciones correspondientes de la lista en el plazo de un mes a partir de la fecha de recepción de la solicitud de la autoridad nacional de supervisión de la certificación.
5. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos de las notificaciones a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 55, apartado 2.

Artículo 53

Grupo Europeo de Certificación de la Ciberseguridad

1. Queda establecido el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»).
2. El Grupo estará integrado por las autoridades nacionales de supervisión de la certificación. Las autoridades estarán representadas por los directores u otros representantes de alto nivel de las autoridades nacionales de supervisión de la certificación.
3. El Grupo desempeñará las siguientes tareas:
 - a) asesorar y asistir a la Comisión en su labor de garantizar la coherencia en la implantación y aplicación del presente título, en particular en relación con las cuestiones de política de certificación de la ciberseguridad, la coordinación de los enfoques políticos y la preparación de los regímenes europeos de certificación de la ciberseguridad;

- b) asistir, asesorar y cooperar con ENISA en relación con la preparación de una propuesta de régimen, de conformidad con el artículo 44 del presente Reglamento;
 - c) proponer a la Comisión que solicite a la Agencia que prepare una propuesta de régimen europeo de certificación de la ciberseguridad de conformidad con el artículo 44 del presente Reglamento;
 - d) adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los regímenes europeos de certificación de la ciberseguridad existentes;
 - e) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar buenas prácticas sobre los regímenes de certificación de la ciberseguridad;
 - f) facilitar la cooperación entre las autoridades nacionales de supervisión de la certificación en virtud del presente título mediante el intercambio de información, y en particular mediante el establecimiento de métodos para un intercambio de información eficaz en relación con todos los temas relacionados con la certificación de la ciberseguridad.
4. La Comisión presidirá el Grupo y se hará cargo de su secretaría, con la asistencia de ENISA según lo previsto en el artículo 8, letra a).

Artículo 54

Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables a los incumplimientos del presente título y de los regímenes europeos de certificación de la ciberseguridad y adoptarán toda medida necesaria para garantizar su aplicación. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias. Los Estados miembros notificarán a la Comisión [a más tardar el .../sin demora] dicho régimen y dichas medidas, así como cualquier modificación posterior que les afecte.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 55

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento (UE) n.º 182/2011.

Artículo 56

Evaluación y revisión

1. A más tardar cinco años después de la fecha a que se refiere el artículo 58, y posteriormente cada cinco años, la Comisión evaluará el impacto, la eficacia y la eficiencia de la Agencia y de sus prácticas de trabajo, así como la posible necesidad de modificar su mandato y las repercusiones financieras que tendría la eventual modificación. La evaluación tomará en consideración los comentarios llegados a la Agencia en respuesta a sus actividades. Si la Comisión considerara que la continuidad de la Agencia ha dejado de estar justificada con respecto a los objetivos, mandato y tareas que le fueron atribuidos, podrá proponer que se modifique el presente Reglamento en lo que se refiere a las disposiciones relacionadas con la Agencia.
2. La evaluación valorará también el impacto, la eficacia y la eficiencia de las disposiciones del título III en relación con los objetivos de garantizar un nivel adecuado de ciberseguridad de los productos y servicios de TIC en la Unión y de mejorar el funcionamiento del mercado interior.
3. La Comisión remitirá el informe de evaluación, conjuntamente con sus conclusiones, al Parlamento Europeo, al Consejo y al Consejo de Administración. Los resultados de dicho informe se harán públicos.

Artículo 57

Derogación y sucesión

1. Queda derogado el Reglamento (CE) n.º 526/2013, con efecto desde el [...].
2. Las referencias al Reglamento (CE) n.º 526/2013 y a ENISA se entenderán hechas al presente Reglamento y a la Agencia.
3. La Agencia será considerada sucesora de la establecida por el Reglamento (CE) n.º 526/2013 en todo lo que se refiere a propiedad, acuerdos, obligaciones legales, contratos de empleo, compromisos financieros y responsabilidades. Todas las decisiones existentes del Consejo de Administración y del Comité Ejecutivo seguirán

siendo válidas, a condición de que no sean incompatibles con las disposiciones del presente Reglamento.

4. La Agencia se establece por un período indefinido a partir del [...].
5. El director ejecutivo nombrado de conformidad con el artículo 24, apartado 4, del Reglamento (CE) n.º 526/2013 será el director ejecutivo de la Agencia para el resto de su mandato.
6. Los miembros del Consejo de Administración designados de conformidad con el artículo 6 del Reglamento (CE) n.º 526/2013 y sus suplentes serán los miembros y sus suplentes del Consejo de Administración de la Agencia para el resto de su mandato.

Artículo 58

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.
2. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo
El Presidente

Por el Consejo
El Presidente

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

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 en las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

1.2. Ámbito(s) político(s) afectado(s)

Ámbito político: 09 - Redes de comunicaciones, contenidos y tecnología

Actividad: 09.02 - Mercado único digital

1.3. Naturaleza de la propuesta/iniciativa

☒ La propuesta/iniciativa se refiere a **una acción nueva (título III – Certificación)**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**⁴³

☒ La propuesta/iniciativa se refiere a **la prolongación de una acción existente (título II – mandato de ENISA)**

☐ 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. Aumentar la resiliencia de los Estados miembros, las empresas y el conjunto de la UE
2. Garantizar el buen funcionamiento del mercado interior de productos y servicios de TIC de la UE
3. Aumentar la competitividad global de las empresas de la UE que operan en el ámbito de las TIC.
4. Aproximar las disposiciones legales, reglamentarias y administrativas de los Estados miembros que exijan ciberseguridad.

1.4.2. Objetivo(s) específico(s)

Teniendo en mente los objetivos generales, en el contexto más amplio de la revisión de la Estrategia de Ciberseguridad, el instrumento, delimitando el ámbito de actuación y el mandato de ENISA y estableciendo el marco europeo para la certificación de productos y servicios de TIC, se propone alcanzar los siguientes objetivos específicos:

1. Aumentar **las capacidades y la preparación** de los Estados miembros y de las empresas.
2. Mejorar **la cooperación y la coordinación** entre los Estados miembros y las instituciones, órganos y organismos de la UE.
3. Aumentar **las capacidades a nivel de la UE para complementar la acción de los**

⁴³

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

Estados miembros, en particular en caso de ciber crisis transfronteriza.

4. Aumentar **la sensibilización** de ciudadanos y empresas sobre las cuestiones relacionadas con la ciberseguridad.
5. Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la **transparencia global de la garantía de ciberseguridad**⁴⁴ de los productos y servicios de TIC.

ENISA contribuirá a la consecución de los citados objetivos mediante:

La mejora del apoyo a la formulación de políticas: Facilitar orientaciones y asesoramiento a la Comisión y a los Estados miembros para actualizar y desarrollar un marco normativo holístico en el ámbito de la ciberseguridad, así como políticas sectoriales e iniciativas legales cuando estén presentes cuestiones relacionadas con la ciberseguridad; contribuir a los trabajos del Grupo de cooperación (artículo 11 de la Directiva (UE) 2016/1148), ofreciendo asesoramiento y asistencia; apoyar el desarrollo y la aplicación de políticas en el ámbito de la identidad electrónica y los servicios de confianza; promover el intercambio de las mejores prácticas entre las autoridades competentes.

La mejora del apoyo a la creación de capacidades: Prestar apoyo a los Estados miembros y a las instituciones, órganos y organismos de la Unión para desarrollar y mejorar la prevención, la detección y el análisis, así como la capacidad para responder a los problemas e incidentes de ciberseguridad; ayudar a los Estados miembros, a petición suya, en el desarrollo de CSIRT nacionales y de estrategias nacionales de ciberseguridad; ayudar a las instituciones de la Unión en la elaboración y revisión de las estrategias de ciberseguridad de la Unión; organizar formación en materia de ciberseguridad; ayudar a los Estados miembros, a través del Grupo de cooperación, en el intercambio de mejores prácticas; facilitar la creación de centros sectoriales de puesta en común y análisis de la información (ISAC).

El apoyo a la cooperación operativa y la gestión de crisis: Apoyar la cooperación entre los organismos públicos competentes y entre las partes interesadas mediante el establecimiento de una cooperación sistemática con las instituciones, órganos y organismos de la Unión que se ocupan de la ciberseguridad, la ciberdelincuencia y la protección de la intimidad y de los datos personales; encargarse de la secretaría de la red de CSIRT (artículo 12, apartado 2, de la Directiva (UE) 2016/1148) y contribuir a la cooperación operativa dentro de la red, prestando, en cooperación con el CERT-UE, apoyo a los Estados miembros, a petición suya; organizar periódicamente ejercicios de ciberseguridad; contribuir al desarrollo de una respuesta cooperativa a los incidentes y crisis de ciberseguridad transfronterizas y a gran escala; llevar a cabo, en cooperación con la red de CSIRT, investigaciones técnicas *ex post* sobre los incidentes importantes y emitir recomendaciones de seguimiento.

Las tareas relacionadas con el mercado (normalización, certificación): Desempeñar una serie de funciones que respalden específicamente el mercado interior: «observatorio del mercado» de la ciberseguridad, analizando las tendencias pertinentes en dicho mercado para adecuar mejor la oferta y la demanda; apoyar y promover el desarrollo y la aplicación de la política de la Unión sobre certificación de la ciberseguridad de productos y servicios de TIC, preparando propuestas de regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, encargándose de la secretaría del Grupo de Certificación

⁴⁴

La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

de la Ciberseguridad de la Unión y proporcionando directrices y buenas prácticas relativas a los requisitos de seguridad de los productos y servicios de TIC en cooperación con las autoridades nacionales de supervisión de la certificación y la industria. **Un mayor apoyo a los conocimientos, la información y la sensibilización:** Prestar asistencia y asesorar a la Comisión y a los Estados miembros para alcanzar un elevado nivel de conocimientos, en toda la Unión, sobre las cuestiones relacionadas con la SRI y su aplicación a las partes interesadas de la industria. Esto supone también la puesta en común, la organización y la puesta a disposición del público, a través de un portal asignado a este propósito, de información sobre seguridad de las redes y los sistemas de información [o ciberseguridad]. Otro elemento importante son las actividades de sensibilización y campañas de información destinadas al público en general sobre los riesgos en materia de ciberseguridad.

Un mayor apoyo a la investigación y la innovación: Proporcionar asesoramiento sobre las necesidades de investigación y el establecimiento de prioridades en el ámbito de la ciberseguridad.

El apoyo a la cooperación internacional: Apoyar los esfuerzos de la Unión por cooperar con terceros países y con organizaciones internacionales a fin de promover la cooperación internacional en materia de ciberseguridad.

CERTIFICACIÓN

El marco de certificación contribuirá al logro de los objetivos incrementando la transparencia general de la garantía de ciberseguridad⁴⁵ de los productos y servicios de TIC y, por ende, reforzando la confianza en el mercado único digital y en la innovación digital. Esto contribuirá también a evitar la fragmentación de los regímenes de certificación en la UE, así como de los requisitos de seguridad y criterios de evaluación conexos en los distintos Estados miembros y sectores.

1.4.3. Resultado(s) e incidencia esperados

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

Se espera que una ENISA reforzada, que preste apoyo a las capacidades, la prevención, la cooperación y la sensibilización a nivel de la UE, diseñada por tanto para aumentar la ciberresiliencia global de la UE, y respalde asimismo el marco europeo de certificación de productos y servicios de TIC tenga los efectos siguientes (lista no exhaustiva):

Impacto global:

- Impacto positivo global sobre el mercado interior gracias a la reducción de la fragmentación del mercado y el aumento de la confianza en las tecnologías digitales a través de una mejor cooperación, unos enfoques más armonizados con respecto a las políticas de ciberseguridad de la UE y unas mayores capacidades a nivel de la UE. Todo ello debería dar lugar a un impacto económico positivo, ya que permitirá reducir los costes de los incidentes relacionados con la ciberseguridad / ciberdelincuencia, estimándose el impacto económico en la Unión en el 0,41 % del PIB de la UE (es decir, en torno a 55 000 millones EUR).

⁴⁵

La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

Resultados específicos:

Aumento de las capacidades y la preparación de los Estados miembros y de las empresas

- Mejora de las capacidades y la preparación de los Estados miembros en materia de ciberseguridad (gracias a análisis estratégicos a largo plazo de las ciberamenazas y los ciberincidentes, orientaciones e informes, intermediación de conocimientos especializados y buenas prácticas, disponibilidad de formación y materiales de formación, refuerzo de los ejercicios CyberEurope).
- Mejora de las capacidades de los agentes privados gracias al apoyo al establecimiento de Centros de puesta en común y análisis de la información (ISAC) en varios sectores.
- Mejora de la preparación en materia de ciberseguridad de la UE y los Estados miembros gracias a la disponibilidad de planes concertados y bien ensayados en caso de incidente de ciberseguridad transfronterizo a gran escala objeto de los ejercicios CyberEurope.

Mejora de la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE

- Mejora de la cooperación tanto dentro de los sectores público y privado como entre ellos.
- Mejora de la coherencia del enfoque con respecto a la aplicación de la Directiva SRI a través de fronteras y sectores.

- Mejora de la cooperación en el ámbito de la certificación, gracias a un marco institucional que permite el desarrollo de regímenes europeos de certificación de la ciberseguridad, así como de una política común en la materia.

Aumento de las capacidades a nivel de la UE para complementar la acción de los Estados miembros

- Mejora de la «capacidad operativa de la UE» para complementar la acción de los Estados miembros y apoyarlos, a petición suya y en relación con servicios limitados y previamente definidos. Se espera que esto tenga un efecto positivo sobre el éxito de la prevención, detección y respuesta a incidentes tanto a nivel de Estado miembro como de la Unión.

Aumento de la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad

- Mejora de los conocimientos generales de ciudadanos y empresas sobre las cuestiones relacionadas con la ciberseguridad.
- Mejora de la capacidad para tomar decisiones con conocimiento de causa sobre la compra de productos y servicios de TIC gracias a la certificación de la ciberseguridad

Fortalecimiento de la confianza en el mercado único digital y en la innovación digital mediante una mayor transparencia de la garantía de ciberseguridad de los productos y servicios de TIC

- Aumento de la transparencia de la garantía de ciberseguridad⁴⁶ de los productos y servicios de TIC gracias a la simplificación de los procedimientos para la certificación de la seguridad aportada por un marco común para la UE.
- Mejora del nivel de garantía de las propiedades de seguridad de los productos y servicios de TIC.

⁴⁶

La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

- Aumento de la utilización de la certificación de la seguridad incentivada por los procedimientos simplificados, la reducción de costes y una perspectiva de oportunidades de negocio a escala de la UE que no se ve afectada por la fragmentación del mercado.

- Mejora de la competitividad dentro del mercado de la ciberseguridad de la UE debida a la reducción de los costes y la carga administrativa para las pymes y a la eliminación de las posibles barreras a la entrada en el mercado causadas por los diversos sistemas de certificación nacionales.

Otros

- No se espera ningún impacto medioambiental significativo en relación con alguno de los objetivos.

- Con respecto al presupuesto de la UE, caben esperar mejoras de la eficiencia derivadas de la mayor cooperación y coordinación de las actividades entre las instituciones, órganos y organismos de la UE.

1.4.4. Indicadores de resultados e incidencia

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

a)

Objetivo: Aumentar las capacidades y la preparación de los Estados miembros y de las empresas:

- Número de sesiones de formación organizadas por ENISA
- Cobertura geográfica (número de países y zonas) de la asistencia directa facilitada por ENISA
- Nivel de preparación alcanzado por los Estados miembros en términos de madurez de los CSIRT y supervisión de las medidas reguladoras relacionadas con la ciberseguridad
- Número de buenas prácticas a escala de la UE para las infraestructuras críticas proporcionadas por ENISA
- Número de buenas prácticas a escala de la UE para las pymes proporcionadas por ENISA
- Publicación por ENISA de análisis estratégicos anuales de las ciberamenazas y los ciberincidentes a fin de detectar tendencias emergentes
- Contribución sistemática de ENISA a la actividad de los grupos de trabajo sobre ciberseguridad de los organismos europeos de normalización.

Objetivo: Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE:

- Número de Estados miembros que han hecho uso de las recomendaciones y dictámenes de ENISA en su proceso de formulación de políticas
- Número de instituciones, órganos y organismos de la UE que han hecho uso de las recomendaciones y dictámenes de ENISA en su proceso de formulación de políticas
- Aplicación sistemática del programa de trabajo de la red de CSIRT y buen

funcionamiento de la infraestructura de TI y los canales de comunicación de la red de CSIRT

- Número de informes técnicos puestos a disposición del Grupo de cooperación y utilizados por él
- Coherencia del enfoque con respecto a la aplicación de la Directiva SRI a través de fronteras y sectores
- Número de evaluaciones del cumplimiento de la reglamentación realizadas por ENISA
- Número de ISACS existentes en los diferentes sectores, en particular para las infraestructuras críticas
- Creación y gestión ordinaria de la plataforma de información que difunde información sobre ciberseguridad procedente de las instituciones, órganos y organismos de la UE
- Contribución sistemática a la preparación de los programas de trabajo de investigación e innovación de la UE
- Acuerdo de cooperación entre ENISA, EC3 y CERT-UE vigente
- Número de regímenes de certificación incluidos y desarrollados con arreglo al marco.

Objetivo: Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de ciber crisis transfronteriza:

- Publicación por ENISA de análisis estratégicos anuales de las ciberamenazas y los ciberincidentes a fin de detectar tendencias emergentes
- Publicación de información agregada de los incidentes notificados en virtud de la Directiva SRI por ENISA
- Número de ejercicios paneuropeos coordinados por la Agencia y número de Estados miembros y organizaciones participantes
- Número de solicitudes de apoyo a la respuesta de emergencia formuladas por los Estados miembros a ENISA y realizadas por la Agencia
- Número de análisis de vulnerabilidades, artefactos e incidentes llevados a cabo por ENISA en cooperación con el CERT-UE
- Disponibilidad de informes de situación a escala de la UE sobre la base de la información comunicada a ENISA por los Estados miembros u otras entidades en caso de ciberincidente transfronterizo a gran escala.

Objetivo: Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad:

- Realización sistemática de campañas de sensibilización a escala de la UE y nacional y actualización periódica de los temas en función de las nuevas necesidades de aprendizaje
- Aumento de la ciber sensibilización entre los ciudadanos de la UE
- Realización sistemática de cuestionarios de sensibilización sobre la ciberseguridad y crecimiento a lo largo del tiempo del porcentaje de respuestas correctas
- Publicación periódica de buenas prácticas de ciberseguridad y ciberhigiene dirigida a los empleados y sus organizaciones.

Objetivo: Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la transparencia global de la garantía de ciberseguridad⁴⁷ de los productos y servicios de TIC:

- Número de regímenes que se adhieren al marco de la UE
- Reducción de los costes de obtención de un certificado de seguridad de las TIC
- Número de organismos de evaluación de la conformidad especializados en certificación de las TIC en los Estados miembros
- Creación del Grupo Europea de Certificación de la Ciberseguridad y organización de sus reuniones
- Directrices para la certificación con arreglo al marco de la UE vigente
- Publicación periódica de análisis de las principales tendencias del mercado de la ciberseguridad en la UE
- Número de productos y servicios de TIC certificados de conformidad con las normas del marco europeo de certificación de la seguridad de las TIC
- Aumento del número de usuarios finales que conocen las características de seguridad de los productos y servicios de TIC

b)

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

Habida cuenta de los requisitos reglamentarios y de la rápida evolución del panorama de las amenazas a la ciberseguridad, es preciso revisar el mandato de ENISA para establecer un nuevo conjunto de tareas y funciones, con vistas a apoyar de manera efectiva y eficaz los esfuerzos de los Estados miembros, las instituciones de la UE y otras partes interesadas para garantizar la seguridad del ciberespacio en la Unión Europea. Se delinea el alcance propuesto del mandato, que refuerza los ámbitos en los que la agencia ha mostrado un claro valor añadido y añade otros nuevos en los que se necesita apoyo a la vista de los nuevos instrumentos y prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el plan director de ciberseguridad de la UE para la cooperación en caso de ciber crisis y la certificación de seguridad de las TIC. El nuevo mandato propuesto intenta atribuir a la Agencia funciones más sólidas y centrales, en particular respaldando también de manera más activa a los Estados miembros para hacer frente a amenazas específicas (capacidad operativa) y convirtiéndose en un centro de conocimientos especializados que asista a los Estados miembros y la Comisión en el ámbito de la certificación de la ciberseguridad.

Al mismo tiempo, la propuesta establece un marco europeo de certificación de la ciberseguridad para los productos y servicios de TIC y especifica las funciones y tareas esenciales de ENISA en el ámbito de la certificación de la ciberseguridad. Dicho Marco establece disposiciones y procedimientos comunes que permiten la creación de regímenes de certificación de la ciberseguridad a escala de la UE para productos o servicios de TIC o riesgos de ciberseguridad específicos. La creación de regímenes europeos de certificación de la ciberseguridad de conformidad con el Marco permitirá que los certificados expedidos con arreglo a dichos regímenes obtengan validez y reconocimiento en todos los Estados miembros y se combata la fragmentación actual del mercado.

⁴⁷

La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

1.4.6. Valor añadido de la intervención de la Unión

La ciberseguridad es un problema verdaderamente global, transfronterizo por naturaleza e intersectorial cada vez en mayor medida debido a las interdependencias entre las redes y los sistemas de información. El número, complejidad y envergadura de los incidentes de ciberseguridad, así como su impacto en la economía y la sociedad, aumentan con el paso del tiempo, y se espera que sigan haciéndolo en paralelo a la evolución de la tecnología, por ejemplo, la proliferación de la internet de las cosas. Esto implica que no cabe esperar que disminuya en el futuro la necesidad de un mayor esfuerzo común de los Estados miembros, las instituciones de la UE y las partes interesadas del sector privado para hacer frente a las amenazas a la ciberseguridad.

Desde su creación en 2004, ENISA ha tratado de fomentar la cooperación entre los Estados miembros y las partes interesadas en el ámbito de los SRI, incluyendo el apoyo a la cooperación entre los sectores público y privado. Este apoyo a la cooperación ha incluido el trabajo técnico encaminado a construir una imagen del panorama de las amenazas a escala de la UE, la creación de grupos de expertos y la organización de ejercicios paneuropeos de gestión de crisis y ciberincidentes para los sectores público y privado (en particular «Cyber Europe»). La Directiva SRI encomendó a ENISA tareas adicionales, incluida la secretaría de la red de CSIRT para la cooperación operativa entre los Estados miembros.

El valor añadido de la actuación a nivel de la UE, en particular para reforzar la cooperación entre los Estados miembros, pero también entre las comunidades SRI, fue reconocido en las Conclusiones del Consejo⁴⁸ de 2016 y también se desprende claramente de la evaluación de ENISA de 2017, que muestra que el valor añadido de la Agencia reside principalmente en su capacidad para fomentar la cooperación entre estas partes interesadas. No existe ningún otro agente a nivel de la UE que facilite la cooperación de una variedad análoga de partes interesadas en la seguridad de las redes y de la información.

El valor añadido de ENISA para acercar a las comunidades de ciberseguridad y las partes interesadas es similar en el ámbito de la certificación. El aumento de la ciberdelincuencia y de las amenazas a la seguridad ha dado lugar a la aparición de iniciativas nacionales que fijan requisitos de alto nivel en materia de certificación y ciberseguridad para los componentes de TIC utilizados en las infraestructuras tradicionales. Si bien estas iniciativas son importantes, conllevan el riesgo de provocar la fragmentación del mercado único y crear obstáculos a la interoperabilidad. Un proveedor de TIC podría tener que someterse a varios procesos de certificación si desea vender en diferentes Estados miembros. Es improbable que la ineficacia o ineficiencia de los actuales regímenes de certificación se corrija en ausencia de intervención de la UE. En ausencia de medidas, es muy probable que la fragmentación del mercado aumente en el corto a medio plazo (próximos 5-10 años) con la aparición de nuevos regímenes de certificación. La falta de coordinación y de interoperabilidad entre dichos regímenes es un elemento que reduce el potencial del mercado único digital. Esto demuestra el valor añadido de la creación de un marco europeo de certificación de la ciberseguridad para productos y servicios de TIC que instaure las condiciones adecuadas para abordar eficazmente el problema relacionado con la coexistencia de múltiples procedimientos de certificación en varios Estados miembros, reduciendo los costes de la certificación y haciendo que esta resulte más

⁴⁸Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

1.4.7. *Principales conclusiones extraídas de experiencias similares anteriores*

De conformidad con la base jurídica de ENISA, la Comisión llevó a cabo una evaluación de la Agencia, que incluía un estudio independiente y una consulta pública. La evaluación llegó a la conclusión de que los objetivos de ENISA siguen siendo pertinentes en la actualidad. En un contexto de avances tecnológicos, evolución de las amenazas y creciente necesidad de una mayor seguridad de las redes y la información (SRI) en la UE, es preciso disponer de conocimientos técnicos sobre la evolución de las cuestiones relativas a la seguridad de las redes y de la información. Deben desarrollarse en los Estados miembros capacidades que permitan comprender las amenazas y responder a ellas, y es precisa una cooperación de las partes interesadas de todos los ámbitos temáticos e instituciones.

La Agencia ha contribuido con éxito al refuerzo de la SRI en Europa merced a la oferta de creación de capacidades en 28 Estados miembros, la mejora de la cooperación entre los Estados miembros y las partes interesadas en la SRI; y la oferta de conocimientos especializados, creación de comunidades y apoyo a la política.

Aun cuando ENISA consiguió dejar su huella, al menos en cierta medida, en el amplio campo de la SRI, no ha conseguido plenamente desarrollar una imagen sólida ni obtener visibilidad suficiente para ser reconocida como «el» centro de conocimientos especializados en Europa. La explicación reside en la amplitud de su mandato, que no estuvo acompañado de unos recursos de proporción pareja. Además, ENISA es la única agencia de la UE cuyo mandato es de duración determinada, lo que limita su capacidad para desarrollar una visión a largo plazo y apoyar a sus partes interesadas de manera sostenible. Esto contrasta también con las disposiciones de la Directiva SRI, que atribuye a ENISA tareas sin señalar fecha de finalización.

En lo que respecta a la certificación de la ciberseguridad de los productos y servicios de TIC, no existe en la actualidad ningún marco europeo. No obstante, el aumento de la ciberdelincuencia y de las amenazas a la seguridad ha dado lugar a la aparición de iniciativas nacionales, que entrañan el riesgo de fragmentación del mercado único.

1.4.8. *Compatibilidad y posibles sinergias con otros instrumentos adecuados*

La iniciativa es sumamente coherente con las políticas existentes, en particular en el ámbito del mercado interior. En efecto, está concebida ateniéndose al enfoque global con respecto a la ciberseguridad, tal como se define en la revisión de la Estrategia para el Mercado Único Digital, a fin de complementar un conjunto completo de medidas, tales como la revisión de la Estrategia de Ciberseguridad de la UE, el plan director de cooperación en caso de ciber crisis y las iniciativas para luchar contra la ciberdelincuencia. Garantizaría la armonía con las disposiciones de la actual legislación en materia de ciberseguridad, en particular la Directiva SRI, y se apoyaría en ella para reforzar la ciberresiliencia de la UE mediante la mejora de las capacidades, la cooperación, la gestión de riesgos y la ciber sensibilización.

Las medidas sobre certificación propuestas deberían combatir la fragmentación potencial ocasionada por los regímenes nacionales de certificación existentes y nuevos, contribuyendo al mismo tiempo al desarrollo del mercado único digital. La iniciativa también sostiene y complementa la aplicación de la Directiva SRI, proporcionando a las empresas sometidas a ella una herramienta muy útil para demostrar el cumplimiento de sus requisitos en el conjunto de la Unión.

El marco europeo de certificación de la ciberseguridad de las TIC propuesto se entiende sin perjuicio del Reglamento general de protección de datos (RGPD)⁴⁹ ni, en particular, de las disposiciones pertinentes en materia de certificación⁵⁰ aplicables a la seguridad del tratamiento de los datos personales. Por último, los regímenes propuestos en el futuro marco europeo deberían basarse en la medida de lo posible en normas internacionales como forma de evitar la creación de obstáculos para el comercio y de garantizar la coherencia con las iniciativas internacionales.

⁴⁹ Reglamento (UE) 2016/679, 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).

⁵⁰ Como los artículos 42 (certificación) y 43 (organismos de certificación), así como los artículos 57, 58, y 70 que se refieren respectivamente a las funciones y competencias de las autoridades independientes de supervisión y las tareas del Comité Europeo de Protección de Datos.

1.5. Duración e incidencia financiera

☐ Propuesta/iniciativa de **duración limitada**

- ☐ Propuesta/iniciativa en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA
- ☐ Incidencia financiera desde AAAA hasta AAAA

☒ Propuesta/iniciativa de **duración ilimitada**

- Ejecución: fase de puesta en marcha desde 2019 hasta 2020,
- y pleno funcionamiento a partir de la última fecha.

1.6. Modo(s) de gestión previsto(s)⁵¹

☒ **Gestión directa** a cargo de la Comisión (título III – Certificación)

- ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

☒ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

- ☐ organizaciones internacionales y sus agencias (especifíquense);
- ☐ el BEI y el Fondo Europeo de Inversiones;
- ☒ los organismos a que se hace referencia en los artículos 208 y 209 (título II — ENISA);
- ☐ 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.

Observaciones

El Reglamento incluye:

- el título II del Reglamento propuesto revisa el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), atribuyéndole un papel importante en la certificación, mientras que
- el título III establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, en el que ENISA desempeña un papel fundamental.

⁵¹ Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

El seguimiento se iniciará inmediatamente después de la adopción del instrumento jurídico y se centrará en su aplicación. La Comisión organizará reuniones con ENISA, representantes de los Estados miembros (por ejemplo, grupo de expertos) y partes interesadas pertinentes, en particular para facilitar la aplicación de las normas relativas a la certificación, como la creación del Consejo.

La primera evaluación tendrá lugar cinco años después de la entrada en vigor del instrumento jurídico, siempre que se disponga de datos suficientes. El instrumento jurídico incluye una cláusula explícita de evaluación y revisión [artículo XXX], en virtud de la cual la Comisión llevará a cabo una evaluación independiente. Posteriormente, la Comisión informará al Parlamento Europeo y al Consejo de su evaluación, adjuntando cuando proceda una propuesta de revisión, a fin de medir el impacto del Reglamento y su valor añadido. Las ulteriores evaluaciones deben tener lugar cada cinco años. Se aplicará la metodología de evaluación contenida en el Reglamento sobre la mejora de la legislación de la Comisión. Estas evaluaciones se llevarán a cabo con la ayuda de estudios específicos, debates de expertos y amplias consultas a las partes interesadas.

El director ejecutivo de ENISA debe presentar cada dos años al Consejo de Administración una evaluación *ex post* de las actividades de ENISA. La Agencia debe, asimismo, elaborar un plan de acción para el seguimiento de las conclusiones de las evaluaciones retrospectivas e informar cada dos años a la Comisión sobre los progresos realizados. El Consejo de Administración debe responsabilizarse de vigilar el seguimiento adecuado de dichas conclusiones.

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

Las fuentes de datos para el seguimiento previsto serían principalmente ENISA, el Grupo Europeo de Certificación de la Ciberseguridad, el Grupo de Cooperación, la red de CSIRT y las autoridades de los Estados miembros. Además de los datos que se derivan de los informes (incluidos los informes anuales de actividad) de ENISA, el Grupo Europeo de Certificación de la Ciberseguridad, el Grupo de Cooperación y la red de CSIRT, se utilizarán instrumentos específicos de recogida de datos cuando sea necesario (por ejemplo, encuestas a las autoridades nacionales, Eurobarómetro e informes de la campaña del mes de la ciberseguridad y los ejercicios paneuropeos).

2.2. Sistema de gestión y de control

2.2.1. Riesgo(s) definido(s)

Los riesgos definidos son limitados: existe ya una agencia de la Unión, cuyo mandato se precisará, reforzando los ámbitos en los que ha mostrado un claro valor añadido y añadiendo otros nuevos en los que es necesario un apoyo a la vista de los nuevos instrumentos y

prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el inminente plan director de ciberseguridad de la UE para la cooperación en caso de ciber crisis y la certificación de seguridad de las TIC.

La propuesta, por tanto, detalla las funciones de la Agencia y propicia mejoras de la eficiencia. El incremento de competencias operativas y tareas no representa un riesgo real en la medida en que complementaría la acción de los Estados miembros y les prestaría apoyo, previa solicitud y en relación con servicios limitados y previamente determinados.

Además, el modelo de agencia propuesto, tal como se establece en el Enfoque Común, garantiza la existencia de un control suficiente para asegurarse de que ENISA trabaja por el logro de sus objetivos. Los riesgos operativos y financieros de los cambios propuestos parecen limitados.

Al mismo tiempo, es necesario garantizar los recursos financieros adecuados para que ENISA pueda cumplir las tareas encomendadas por el nuevo mandato, en particular en el ámbito de la certificación.

2.2.2. *Método(s) de control previsto(s)*

Las cuentas de la agencia se someterán a la aprobación del Tribunal de Cuentas y al procedimiento de aprobación de la gestión, estando previstas auditorías.

Todas sus operaciones estarán sujetas a la supervisión del Defensor del Pueblo Europeo de conformidad con lo dispuesto en el artículo 228 del Tratado.

Véanse asimismo los puntos 2.1 y 2.2.1.

2.3. **Medidas de prevención del fraude y de las irregularidades**

Especifíquense las medidas de prevención y protección existentes o previstas.

Medidas de prevención y protección de ENISA que se aplicarán:

- El personal de la Agencia inspecciona los pagos efectuados por cualquier servicio o estudio antes de que se proceda a ningún desembolso, teniendo en cuenta las obligaciones contractuales, los principios económicos y las buenas prácticas financieras y de gestión. En todos los acuerdos y contratos celebrados entre la Agencia y los beneficiarios de pagos se incluirán disposiciones antifraude (supervisión, requisitos de información, etc.).
- Para combatir el fraude, la corrupción y otras actividades ilegales, se aplicará sin restricción lo dispuesto en el Reglamento (CE) n° 883/2013 del Parlamento Europeo y del Consejo, de 25 de mayo de 1999, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).
- La Agencia suscribirá, en un plazo de seis meses a partir del día de entrada en vigor del Reglamento, el 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), y adoptará sin demora las disposiciones apropiadas, que serán de aplicación a todo el personal de la Agencia.

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)

- Líneas presupuestarias existentes

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			
		CD/CND ⁵²	de países de la AELC ⁵³	de países candidatos ⁵⁴	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
1a Competitividad para el crecimiento y el empleo	09.0203 ENISA y certificación de seguridad de las tecnologías de la información y las comunicaciones	CD	SÍ	NO	NO	NO
5 Gastos administrativos]	09.0101 Gastos de personal en activo de la DG de Redes de comunicaciones, contenidos y tecnología 09.0102 Gastos de personal externo en activo de la DG de Redes de comunicaciones, contenidos y tecnología	CND	NO	NO	NO	NO

⁵² CD = créditos disociados / CND = créditos no disociados.

⁵³ AELC: Asociación Europea de Libre Comercio.

⁵⁴ Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

	09.010211 Otros gastos de gestión					
--	-----------------------------------	--	--	--	--	--

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		1a	Competitividad para el crecimiento y el empleo					
ENISA			Base de referenci a 2017 (31.12.2016)	2019 (a partir del 1.7.2019)	2020	2021	2022	TOTAL
Título 1: Gastos de personal <i>(incluidos también los gastos relacionados con la contratación de personal, la formación, la infraestructura y los servicios externos)</i>	Compromisos	(1)	6,387	9,899	12,082	13,349	13,894	49,224
	Pagos	(2)	6,387	9,899	12,082	13,349	13,894	49,224
Título 2: Gastos de infraestructura y funcionamiento	Compromisos	(1a)	1,770	1,957	2,232	2,461	2,565	9,215
	Pagos	(2 a)	1,770	1,957	2,232	2,461	2,565	9,215
Título 3: Gastos de operaciones	Compromisos	(3a)	3,086	4,694	6,332	6,438	6,564	24,028
	Pagos	(3b)	3,086	4,694	6,332	6,438	6,564	24,028
TOTAL de los créditos para ENISA	Compromisos	=1+1 a +3a	11,244	16,550	20,646	22,248	23,023	82,467
	Pagos	=2+2 a +3b	11,244	16,550	20,646	22,248	23,023	82,467

Rúbrica del marco financiero plurianual	5	«Gastos administrativos»
--	----------	--------------------------

En millones EUR (al tercer decimal)

		2019 <i>(a partir del 1.7.2019)</i>	2020	2021	2022	TOTAL
DG: CNECT						
• Recursos humanos		0,216	0,846	0,846	0,846	2,754
• Otros gastos administrativos		0,102	0,235	0,238	0,242	0,817
TOTAL DG CNECT	Créditos	0,318	1,081	1,084	1,088	3,571

Los costes de personal se han calculado de acuerdo con la fecha prevista de contratación (suponiendo que el empleo comienza el 1.7.2019).

La perspectiva de recursos después de 2020 es indicativa y sin perjuicio de las propuestas de la Comisión para el marco financiero plurianual posterior a 2020.

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	0,318	1,081	1,084	1,088	3,571
--	---	-------	-------	-------	-------	--------------

En millones EUR (al tercer decimal)

		2019	2020	2021	2022	TOTAL
TOTAL de los créditos	Compromisos	16,868	21,727	23,332	24,11	86,038

para las RÚBRICAS 1 a 5 del marco financiero plurianual	Pagos	16,868	21,727	23,332	24,11	86,038
---	-------	--------	--------	--------	-------	---------------

3.2.2. Incidencia estimada en los créditos de la Agencia

- ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.
- ☒ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⁵⁵ ↓	2019	2020	2021	2022	TOTAL
Aumentar las capacidades y la preparación de los Estados miembros y de las empresas	1,408	1,900	1,931	1,969	7,208
Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE	0,939	1,266	1,288	1,313	4,806
Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de ciber crisis transfronterizas	0,704	0,950	0,965	0,985	3,604
Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad	0,704	0,950	0,965	0,985	3,604
Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la transparencia global de la garantía de ciberseguridad de los productos y servicios de TIC	0,939	1,266	1,288	1,313	4,806
COSTE TOTAL	4.694	6,332	6,437	6,565	24,028

⁵⁵ En este cuadro figuran únicamente los gastos operativos del título 3.

3.2.3. Incidencia estimada en los recursos humanos de la Agencia

3.2.3.1. Resumen

- ☐ 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)

	T3/4 2019	2020	2021	2022
Agentes temporales (Categoría AD)	4,242	5,695	6,381	6,709
Agentes temporales (Categoría AST)	1,601	1,998	2,217	2,217
Agentes contractuales	2,041	2,041	2,041	2,041
Expertos nacionales en comisión de servicios	0,306	0,447	0,656	0,796
TOTAL	8,190	10,181	11,295	11,763

Los costes de personal se han calculado de acuerdo con la fecha prevista de contratación (para el personal actual de ENISA se asumió pleno empleo a partir de 1.1.2019). Para el nuevo personal se previó empleo progresivo a partir del 1.7.2019 para alcanzar el pleno empleo en 2022. La perspectiva de recursos después de 2020 es indicativa y sin perjuicio de las propuestas de la Comisión para el marco financiero plurianual posterior a 2020.

Incidencia estimada en el personal (ETC adicionales), plantilla de personal

Categoría y grado	2017 ENISA actual	T3/T4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

Total AD	34	9	8	6	3
AST11					
AST10					
AST9					
AST8					
AST7	2	1	1	1	
AST6	5	2	1		
AST5	5				
AST4	2				
AST3					
AST2					
AST1					
Total AST	14	3	2	1	
AST/SC 6					
AST/SC 5					
AST/SC 4					
AST/SC 3					
AST/SC 2					
AST/SC 1					
Total AST/SC					
TOTAL GENERAL	48	12	10	7	3

Las tareas adicionales del personal AD/AST adicional para la consecución de los objetivos del instrumento, según lo descrito en la sección 1.4.2:

Tareas	AD	AST	ENCS	Total
Política y creación de capacidades	8	1		9
Cooperación operativa	8	1	7	16
Certificación (tareas relacionadas con el mercado)	9	3	2	14
Conocimientos, información y sensibilización	1	1		2
TOTAL	26	6	9	41

Descripción de las tareas que deben llevarse a cabo:

Tareas	Recursos adicionales necesarios
Elaboración y ejecución de las políticas de la UE y creación de capacidades	Las tareas incluirán asistir al Grupo de cooperación, apoyar la aplicación coherente de la SRI a través de las fronteras, presentar periódicamente informes sobre el estado de la aplicación del marco jurídico de la UE; asesorar y coordinar las iniciativas sectoriales de ciberseguridad en sectores como la energía, el transporte (aviación / carretera / marítimo /

	vehículos conectados), salud o finanzas, y prestar apoyo al establecimiento de Centros de puesta en común y análisis de la información (ISAC) en varios sectores.
Cooperación operativa y gestión de crisis	Las tareas incluirían: Encargarse de la secretaría de la red de CSIRT garantizando, entre otras cosas, el buen funcionamiento de las infraestructuras de TI y los canales de comunicación de dicha red. Garantizar una cooperación estructurada con el CERT-UE, EC3 y otros organismos de la UE pertinentes. Organizar ejercicios Cyber Europe⁵⁶ - tareas relativas al paso de un evento bienal a otro anual y garantizar que los ejercicios contemplan los incidentes de principio a fin. Asistencia técnica - Las tareas incluirían una cooperación estructurada con el CERT-UE para proporcionar asistencia técnica en caso de incidentes significativos y para apoyar el análisis de incidentes. Para ello es preciso ofrecer a los Estados miembros asistencia para gestionar incidentes y analizar vulnerabilidades, artefactos e incidentes. Facilitar la cooperación entre Estados miembros concretos en la gestión de la respuesta de emergencia mediante un análisis y agregación de los informes de situación nacionales sobre la base de la información que los Estados miembros y otras entidades pongan a disposición de la Agencia. Plan director para una respuesta coordinada a los ciberincidentes transfronterizos a gran escala - La Agencia contribuirá a desarrollar una respuesta cooperativa, a nivel de la Unión y de los Estados miembros, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad a través de una serie de tareas que van desde contribuir a establecer un conocimiento de la situación a nivel de la Unión hasta someter a prueba los planes de cooperación en caso de incidentes. Investigaciones técnicas ex post sobre los incidentes - Llevar a cabo o participar en

⁵⁶

Cyber Europe es el ejercicio de ciberseguridad más grande y completo de la UE hasta la fecha, con participación de más de 700 profesionales de la ciberseguridad de los 28 Estados miembros. Se celebra cada dos años. La evaluación de ENISA y la Estrategia de Ciberseguridad de la UE de 2013 señalan que muchas partes interesadas abogan por convertir Cyber Europe en un evento anual, habida cuenta de la rápida evolución de las ciberamenazas. Sin embargo, esto no es viable por el momento, teniendo en cuenta los limitados recursos de la Agencia.

	investigaciones técnicas <i>ex post</i> sobre los incidentes en cooperación con la red de CSIRT con vistas a formular recomendaciones y reforzar las capacidades en forma de informes públicos para mejorar la prevención de incidentes futuros.
Tareas relacionadas con el mercado (normalización, certificación)	Las tareas incluirían apoyar activamente el trabajo emprendido en el marco de certificación, incluida la prestación de asesoramiento técnico para preparar propuestas de regímenes europeos de certificación de la ciberseguridad. Las tareas también incluirán el apoyo a la elaboración y aplicación de las políticas de la Unión en materia de normalización, certificación y observatorio del mercado; esto exigirá facilitar la asimilación de las normas de gestión de riesgos de los productos, redes y servicios electrónicos y asesorar a los operadores de servicios esenciales y a los proveedores de servicios digitales sobre requisitos técnicos de seguridad. Las tareas incluirán también un análisis de las principales tendencias del mercado.
Conocimientos e información, sensibilización:	Con el fin de garantizar un acceso más fácil a una información mejor estructurada sobre los riesgos en materia de ciberseguridad y las posibles soluciones, la propuesta confiere a la Agencia la nueva tarea de desarrollar y mantener la «plataforma de información» de la Unión. Se incluirían las tareas de reunir, organizar y poner a disposición del público, a través de un portal asignado a este propósito, información sobre la seguridad de las redes y los sistemas de información facilitada por las instituciones, órganos y organismos de la Unión. También incluiría el apoyo a las actividades de ENISA en el ámbito de la sensibilización para que la Agencia pueda aumentar la magnitud del esfuerzo.

3.2.3.2. Necesidades estimadas de recursos humanos para la DG matriz

- ☐ 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 valores enteros (o, a lo sumo, con un decimal)

		Personal adicional			
	Referencia 2017	T3/4 2019	2020	2021	2022
• Empleos de plantilla (funcionarios y personal temporal)					
09 01 01 01 (Sede y Oficinas de Representación de la Comisión)	1	2	3		
• Personal externo (en unidades de equivalente a jornada completa: EJC)⁵⁷					
09 01 02 01 (AC, ENCS, INT de la dotación global)	1	2			
TOTAL		4	3		

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Representar a la Comisión en el Consejo de Administración de la Agencia. Elaborar el dictamen de la Comisión sobre el documento único de programación de ENISA y supervisar su aplicación. Supervisar la preparación del presupuesto de la Agencia y controlar su ejecución. Asistir a la Agencia en el desarrollo de sus actividades en consonancia con las políticas de la Unión, en particular mediante la participación en las reuniones pertinentes. Supervisar la aplicación del marco para los regímenes europeos de certificación de la ciberseguridad de los productos y servicios de TIC. Mantener contactos con los Estados miembros y otras partes interesadas pertinentes en lo que respecta a la labor de certificación. Cooperar con ENISA en relación con las propuestas de regímenes. Preparar propuestas de regímenes europeos de ciberseguridad.
-----------------------------------	---

⁵⁷

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.

Personal externo	Como en el caso anterior.
------------------	---------------------------

3.2.4. *Compatibilidad con el marco financiero plurianual vigente*

- ☐ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.
- ☒ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

La propuesta implicará la reprogramación del artículo 09 02 03, debido a la revisión del mandato de ENISA, que confiere a la Agencia nuevas tareas relacionadas, entre otras cosas, con la aplicación de la Directiva SRI y del marco europeo de certificación de la ciberseguridad. Importes correspondientes:

Año	Previsión	Solicitud
2019	10,739	16,550
2020	10,954	20,646
2021	N/A	22,248*
2022	N/A	23,023*

* Se trata de una estimación. La financiación de la UE después de 2020 se examinará en el contexto de un debate a nivel de la Comisión sobre todas las propuestas para el período posterior a 2020. Esto significa que, una vez que la Comisión haya formulado su propuesta relativa al próximo marco financiero plurianual, la Comisión presentará una ficha financiera legislativa modificada que tenga en cuenta las conclusiones de la evaluación de impacto⁵⁸.

- ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual⁵⁹.

3.2.5. *Contribución de terceros*

- ☐ La propuesta/iniciativa no prevé la cofinanciación por terceros.
- ☒ La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

⁵⁸ Enlace a la página con la evaluación de impacto

⁵⁹ Véanse los artículos 11 y 17 del Reglamento (UE, Euratom) n.º 1311/2013, por el que se establece el marco financiero plurianual para el período 2014-2020.

	Año 2019	Año 2020	Año 2021	Año 2022
AELC	p.m. ⁶⁰ .	p.m.	p.m.	p.m.

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

⁶⁰ El importe exacto para los años siguientes se conocerá en el momento en que se fije el factor de proporcionalidad de la AELC para el año de que se trate.