Consejo de la Unión Europea

Bruselas, 29 de mayo de 2018
(OR. en)

9350/18

Expediente interinstitucional: 2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTA

De:	Presidencia
A:	Consejo
N.º doc. prec.:	8834/18
N.° doc. Ción.:	12183/17
Asunto:	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») - Orientación general

I. INTRODUCCIÓN

1. El 13 de septiembre de 2017, en el contexto de su Estrategia para el Mercado Único Digital, la Comisión adoptó y transmitió al Consejo y al Parlamento Europeo la propuesta de referencia[1], que tiene por fundamento jurídico el artículo 114 del TFUE. Como parte del denominado «paquete de ciberseguridad», la presente propuesta aspira a un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, con vistas a garantizar el correcto funcionamiento del mercado interior.

2. El Reglamento propuesto establece los objetivos, las funciones y los aspectos organizativos de ENISA (la Agencia de Ciberseguridad de la UE) y crea un marco para la institución 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. La propuesta de la Comisión está acompañada de una evaluación de impacto que estudia un conjunto concreto de ocho posibilidades de medidas, que abarcan la revisión de ENISA y la certificación de ciberseguridad de TIC.

3. El Reglamento propuesto contiene dos vertientes principales:

   - un mandato permanente para la Agencia con un alcance precisado en vista de las necesidades en virtud de los nuevos instrumentos y prioridades políticas y un nuevo conjunto de tareas y funciones para la Agencia, de modo que se dé un apoyo efectivo y eficaz a los esfuerzos de los Estados miembros, las instituciones de la UE y otras partes interesadas al objeto de garantizar la seguridad del ciberespacio.

   - un marco europeo de certificación de la ciberseguridad para los productos y servicios de TIC y las normas que rigen los regímenes europeos de certificación de la ciberseguridad que permiten 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.

[1] Docs. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. En octubre de 2017, el Consejo Europeo[2] instó a que las propuestas de la Comisión sobre ciberseguridad se elaborasen desde una perspectiva de conjunto, se presentasen oportunamente y se examinasen sin demora, con arreglo al plan de acción que establezca el Consejo.

5. El 12 de diciembre de 2017, el Consejo de Asuntos Generales adoptó el Plan de acción[3] para la aplicación de las Conclusiones del Consejo[4] sobre la Comunicación conjunta[5] al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE». El Plan de acción reflejaba la ambición del Consejo de obtener una orientación general sobre la propuesta como muy tarde en junio de 2018.

6. En el Parlamento Europeo se ha designado como ponente a Angelika NIEBLER (ITRE, PPE). La Comisión ITRE tiene previsto votar su informe el 19 de junio de 2018.

7. El Comité Económico y Social adoptó su dictamen el 14 de febrero de 2018.

II. TRABAJOS EN EL CONSEJO

8. La Comisión presentó esta propuesta y su evaluación de impacto en el Grupo Horizontal «Cuestiones Cibernéticas» (en lo sucesivo, «el Grupo») el 26 de septiembre de 2017, y posteriormente el Grupo realizó un examen de la evaluación de impacto el 20 de octubre de 2017. Los debates posteriores se centraron en la capacidad operativa de la Agencia y el alcance de la interacción con las autoridades nacionales competentes, así como sobre las repercusiones del marco de certificación en el mercado y la competitividad de las empresas. En general, las Delegaciones acogieron positivamente la evaluación de impacto y la propuesta.

---

2 EUCO 14/17, punto 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. El debate de la propuesta en sí por el Grupo comenzó en noviembre de 2017 bajo la Presidencia estonia y continuó con la Presidencia búlgara. Se dedicaron doce reuniones a la propuesta, que produjeron ocho versiones revisadas consecutivas de la misma al objeto de acordar una orientación general en el próximo Consejo TTE (Telecomunicaciones) que se celebrará el 8 de junio de 2018.

10. El resultado de los debates en el Grupo celebrados los días 14 y 15 de mayo de 2018, así como del texto transaccional revisado de la Presidencia figura en el anexo a la presente nota. Los considerandos se han adaptado a fin de reflejar los cambios introducidos en la parte dispositiva. Los cambios con respecto a la propuesta de la Comisión se indican en **negrita** o mediante el símbolo […]. Los cambios con respecto al documento más reciente del Grupo (8834/18) se indican en **negrita y subrayado** y todas las supresiones se marcan con el signo **[…]**.

III. CONCLUSIÓN

11. El texto transaccional de la Presidencia, recogido en el anexo, refleja el empeño de la Presidencia y los Estados miembros por conseguir un equilibrio adecuado en el texto.

12. El 25 de mayo de 2018, el Comité de Representantes Permanentes alcanzó un acuerdo sobre el texto transaccional de la Presidencia sujeto a modificaciones en los artículos 19, apartado 5, y 48, apartado 5, que figuran en el anexo.

13. Se ruega, por tanto, al Consejo que adopte una orientación general en su reunión del 8 de junio de 2018 y dé instrucciones a la Presidencia para que entable negociaciones con los representantes del Parlamento Europeo y la Comisión Europea sobre este expediente.

ANEXO

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a ENISA, la «*Agencia […] de la […] Unión Europea para la Ciberseguridad*», 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,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[6],

Visto el dictamen del Comité de las Regiones[7],

De conformidad con el procedimiento legislativo ordinario,

[6] DO C de, p.
[7] DO C de, p.

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 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 460/2004[8] 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 1007/2008[9], que prorrogaba el mandato de la Agencia hasta marzo de 2012. El Reglamento (CE) n.º 580/2011[10] 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 526/2013[11] 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.

---

8 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).

9 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).

10 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).

11 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).

(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 Reglamente 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 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 Unión Europea.

(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 **apoyar** […] los esfuerzos nacionales y **contribuir proactivamente a los** 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 **y sus aspectos sectoriales para potenciar la pertinencia de las políticas y la legislación de la UE con la dimensión de la ciberseguridad y posibilitar la coherencia en su aplicación a nivel nacional** […]. 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 **las ciberamenazas y los ciberincidentes** […], 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. **Las actividades realizadas por ENISA relacionadas con las capacidades operativas de los Estados miembros únicamente deben ser complementarias a las acciones propias emprendidas por los Estados miembros en el cumplimiento de sus obligaciones derivadas de la Directiva SRI y, por tanto, no deben sustituirlas** […].

(15 *bis*) La Agencia debe también prestar asistencia en la elaboración y actualización de las estrategias de la Unión y, previa solicitud, de los Estados miembros 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 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, […] **la Agencia debe** apoyar **la puesta en común de información de forma intra- e intersectorial, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, 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, por ejemplo, facilitando** […] la creación de centros sectoriales de puesta en común y análisis de la información (ISAC, por sus siglas en inglés) […].

(18) La Agencia debe agregar y analizar los informes nacionales de los CSIRT y el CERT-UE **que se compartan de forma voluntaria, a los efectos de prestar asistencia a los Estados miembros para** establecer […] **unos procedimientos**, 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 […] **dentro** 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 transfronterizos a gran escala. Esta función debe **desempeñarse con arreglo a su mandato en virtud del presente Reglamento y una fórmula que acordarán los Estados miembros en el contexto de la Recomendación de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala. Podría** 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 […] **periódicos** de ciberseguridad.

(20) […] **Al apoyar la cooperación operativa**, la Agencia debe hacer uso de las competencias **técnicas y operativas** disponibles del CERT-UE a través de una cooperación estructurada […]. […]Cuando proceda, deben establecerse disposiciones específicas adecuadas entre las dos organizaciones para definir los aspectos prácticos de dicha cooperación **y evitar la duplicación de actividades**.

(21) En cumplimiento de sus tareas […] **de apoyo de la cooperación operativa dentro de la red de CSIRT**, la Agencia debe poder prestar ayuda a los Estados miembros **a solicitud de estos**, por ejemplo, mediante **el** asesoramiento **sobre cómo mejorar sus capacidades para prevenir, detectar y responder ante incidentes, la […] facilitación de la gestión** […] técnica **de incidentes que tengan un impacto significativo o sustancial** […] o **el** análisis de amenazas e incidentes. **La facilitación de la gestión técnica de los incidentes que tengan un impacto significativo o sustancial debe incluir, en particular, que ENISA apoye la puesta en común voluntaria de soluciones técnicas entre Estados miembros o aporte información técnica combinada, como las soluciones técnicas que pongan en común voluntariamente los Estados miembros.** 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 […] **apoyo a la cooperación operativa**.

(22) Dentro de la cooperación regular a nivel técnico para ayudar a la Unión a conocer la situación, la Agencia debe elaborar periódicamente **y en estrecha cooperación con los Estados miembros** 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 […] o los puntos de contacto únicos de la Directiva SRI **(ambos de forma voluntaria)**, 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) **El apoyo de la Agencia a l**[…]as investigaciones técnicas *ex post* en relación con incidentes con efectos significativos […] a petición […] de los Estados miembros afectados […] **debe** centrarse en la prevención de incidentes futuros […]. **Los Estados miembros afectados deben proporcionar la información necesaria para que la Agencia pueda apoyar de forma efectiva la investigación técnica.**

(24) […]

(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 **que esté disponible públicamente o se comparta de forma voluntaria** 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 […] **incidentes de** 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 **ciber**seguridad de […] las infraestructuras […] **prestando apoyo, en particular, a los sectores recogidos en el anexo II de la Directiva SRI y los que utilicen los proveedores de servicios digitales que figuran en el anexo III de dicha Directiva**, 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), la **Agencia del Sistema Global de Navegación por Satélite Europeo (Agencia del GNSS Europeo)** y cualquier otro órgano de la UE relacionado con la seguridad informática. También debe mantener contactos con las autoridades encargadas de la protección de datos a fin de intercambiar conocimientos y mejores prácticas y facilitar asesoramiento sobre los aspectos de la ciberseguridad que podrían repercutir en su trabajo. Los representantes de las autoridades nacionales y de la Unión encargadas de hacer cumplir la ley y proteger los datos deben poder estar representados en el Grupo Permanente de Partes Interesadas de la Agencia. En sus relaciones con los organismos encargados de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en el trabajo de dichos organismos, la Agencia debe respetar los canales de información y las redes existentes.

(31) La Agencia, […] en su función de secretaría de la red de CSIRT, 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 […] **periódicamente** 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 ciberseguridad. **A fin de determinar las necesidades y prioridades en materia de investigación, la Agencia debe consultar asimismo a los grupos de usuarios pertinentes.**

(37) […] **Las amenazas** de ciberseguridad tienen un alcance mundial. Es necesaria una cooperación internacional más estrecha para mejorar las normas de **ciber**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 incluya la aplicación del programa de trabajo anual de la Agencia** 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 Consejo[12]. 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 datos[13]. 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.

---

[12] 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).

[13] DO L 8 de 12.1.2001, p. 1.

(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) […]

(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 **procesos,** 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 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 y **las declaraciones de conformidad de la UE** 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 […] **europeas**, 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 **procesos,** productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales […] de certificación **de la ciberseguridad** 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 **procesos**, productos y servicios de TIC certificados con arreglo a un régimen cumplan los requisitos especificados […] **con** objeto de […] **proteger** la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, procesos, servicios y sistemas **a lo largo de su ciclo de vida**, 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 **procesos,** productos y servicios de TIC. Los **procesos,** 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 **procesos,** productos y servicios de TIC deben especificarse luego con más detalle a nivel de cada régimen de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas **cuando no se disponga de normas apropiadas**.

(55 *bis*) **Las especificaciones técnicas que deben utilizarse en un régimen europeo de certificación de la ciberseguridad deben determinarse a través del cumplimiento de los principios establecidos en el anexo II del Reglamento (UE) 1025/2012. No obstante, podrían considerarse necesarias algunas variaciones con respecto a estos principios en casos debidamente justificados en los que dichas especificaciones técnicas vayan a utilizarse en un régimen europeo de certificación de la ciberseguridad de nivel de garantía elevado. Los motivos que justifican tales variaciones deben hacerse públicos.**

(55 *ter*) **La evaluación certificada de la conformidad es el proceso por el que se evalúa si se han cumplido los requisitos especificados en relación con un proceso, producto o servicio de TIC. Para llevar a cabo este proceso es necesario un tercero independiente, que no sea el fabricante del producto ni el proveedor del servicio. El proceso de expedición de un certificado es posterior al proceso de evaluación positiva de un proceso, producto o servicio de TIC. Debe considerarse una confirmación de que la evaluación correspondiente se ha llevado a cabo de forma apropiada. En función del nivel de garantía, el régimen europeo de ciberseguridad debe determinar si el encargado de expedir el certificado es un organismo público o privado. La evaluación de la conformidad y la certificación no pueden garantizar por sí mismas 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.**

(55 *quater*) **La elección, por parte de los usuarios de certificados, del nivel adecuado de certificación y de los requisitos de seguridad asociados debe basarse en el análisis del riesgo sobre el uso del proceso, producto o servicio de TIC. Por tanto, el nivel de garantía debe ser proporcional al nivel de riesgo asociado con el uso previsto de un proceso, producto o servicio de TIC.**

(55 *quinquies*) Un régimen europeo de certificación de la ciberseguridad podría determinar que la evaluación de la conformidad se realice bajo la responsabilidad exclusiva del fabricante o proveedor de productos y servicios de TIC (autoevaluación de la conformidad). En tales casos, basta con que el fabricante o proveedor lleve a cabo por sí mismo todas las comprobaciones que garanticen la conformidad de los procesos, productos o servicios de TIC con el régimen de certificación. Este tipo de evaluación de la conformidad debe considerarse adecuado para productos y servicios de TIC poco complejos (por ejemplo, cuando el diseño y el mecanismo de producción son sencillos) cuyo nivel de riesgo para el interés público sea bajo. Asimismo, únicamente los productos y servicios de TIC que corresponden al nivel de garantía básico podrían acogerse a la autoevaluación de la conformidad.

(55 *sexies*) Un régimen europeo de certificación de la ciberseguridad podría permitir la autoevaluación tanto de la certificación como de la conformidad de los productos y servicios de TIC. En este caso, el régimen debe establecer medios claros y comprensibles para que los consumidores u otros usuarios puedan diferenciar los productos y servicios evaluados bajo la responsabilidad del fabricante o proveedor de productos y servicios certificados por un tercero.

(55 *septies*) El fabricante o proveedor de productos o servicios de TIC que lleve a cabo una autoevaluación de la conformidad debe redactar y firmar la declaración de conformidad de la UE como parte del procedimiento de evaluación de la conformidad. La declaración de conformidad de la UE es el documento que determina si un producto o servicio de TIC concreto cumple los requisitos del régimen. Al redactar y firmar la declaración de conformidad de la UE, el fabricante o proveedor asume la responsabilidad de que el producto o servicio de TIC cumple los requisitos legales del régimen. Debe presentarse una copia de la declaración de conformidad de la UE a la autoridad nacional de certificación de la ciberseguridad y a ENISA.

(55 *octies*) El fabricante o proveedor de productos y servicios de TIC debe poner a disposición de la autoridad nacional de certificación de la seguridad competente, por un plazo definido en el régimen europeo específico de certificación de la ciberseguridad, la declaración de conformidad de la UE y la documentación técnica de toda la información pertinente relativa a la conformidad de los productos o servicios de TIC con un régimen. La documentación técnica debe especificar los requisitos aplicables y contemplar, en la medida en que sea pertinente para la evaluación, el diseño, la fabricación y el funcionamiento del producto o servicio de TIC. La documentación técnica debe recopilarse de forma tal que permita la evaluación de la conformidad de un producto o servicio de TIC con los requisitos pertinentes.

(55 *nonies*) Los Estados miembros y las organizaciones de partes interesadas deben tener derecho a plantear la preparación de una propuesta de régimen al Grupo Europeo de Certificación de la Ciberseguridad. Las organizaciones de partes interesadas son organizaciones de representantes de la industria o de los consumidores, entre ellos los representantes de las organizaciones de pymes que tienen un interés legítimo en que se desarrolle un régimen europeo de certificación de la ciberseguridad. Dichas propuestas deben analizarse a la luz de los criterios establecidos por el Grupo Europeo de Certificación de la Ciberseguridad con arreglo a unas orientaciones basadas en los principios de transparencia, apertura, imparcialidad, consenso, eficacia, relevancia y coherencia.

(56) La Comisión **y el Grupo** deben estar facultados para solicitar a ENISA que prepare **sin demora indebida** propuestas de regímenes para **procesos**, 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 **procesos,** 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 **y los niveles de evaluación cuando proceda**.

(56 *bis*) La garantía de un régimen europeo de certificación constituye la base para confiar en que un proceso, producto o servicio de TIC cumple los requisitos sobre seguridad de un régimen europeo de certificación de la ciberseguridad específico. Con el fin de garantizar la coherencia del marco sobre procesos, productos y servicios de TIC certificados, un régimen europeo de certificación de la ciberseguridad podría especificar niveles de garantía para los certificados europeos de ciberseguridad y las declaraciones de conformidad de la UE expedidos con arreglo a dicho régimen. Cada certificado podría referirse a uno de los niveles de garantía (básico, sustancial o elevado), mientras que la declaración de conformidad de la UE solo podría referirse al nivel de garantía básico. Los niveles de garantía determinan el nivel de […] dedicación necesario para la evaluación y se definen con referencia a especificaciones técnicas, normas y procedimientos correspondientes, incluidos los controles técnicos, cuyo objeto es reducir o evitar incidentes de ciberseguridad. Cada nivel de garantía debe ser constante en los distintos ámbitos sectoriales a los que se aplica la certificación.

(56 *ter*) Un régimen europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y la profundidad la metodología de evaluación utilizada, que debe equivaler a uno de los niveles de garantía y debe asociarse con una combinación adecuada de componentes de garantía. En todos los niveles de garantía, el producto o servicio de TIC debe contener varias funciones de seguridad, definidas por el régimen, que pueden incluir una configuración innovadora segura, un código firmado, una actualización segura, la reducción de programas intrusos y la protección total de las memorias *stack/heap*. Una vez creadas, dichas funciones deben conservarse utilizando fórmulas de desarrollo centradas en la seguridad e instrumentos asociados para garantizar que se incorporen mecanismos eficaces de forma fiable (tanto *software* como *hardware*) En el caso del nivel de garantía básico, la evaluación debe regirse al menos por los siguientes componentes de garantía: la evaluación debe incluir como mínimo una revisión de la documentación técnica del producto o servicio de TIC por el organismo de evaluación de la conformidad. Cuando la certificación incluya procesos de TIC, también debe someterse a la revisión técnica el proceso utilizado para diseñar, desarrollar y mantener un producto o servicio de TIC. En los casos en que un régimen europeo de certificación de la ciberseguridad establezca una autoevaluación de la conformidad, debe ser suficiente con que el fabricante o proveedor haya llevado a cabo una autoevaluación sobre el cumplimiento de los procesos, productos o servicios de TIC con respecto al régimen de certificación. En el caso del nivel de garantía sustancial, la evaluación, además de cumplir con lo indicado para el nivel de garantía básico, debe regirse por la verificación de la conformidad de las funcionalidades de seguridad del producto o servicio de TIC con respecto a su documentación técnica. Para el nivel de garantía elevado, la evaluación, además de cumplir con lo indicado para el nivel de garantía sustancial, debe regirse por una prueba de eficacia que evalúe la resistencia de las funcionalidades de seguridad del producto o servicio de TIC frente a quienes llevan a cabo ciberataques complejos sirviéndose de habilidades y recursos significativos.

(56 *quater*) A la hora de preparar una propuesta de régimen, ENISA debe consultar a todas las partes interesadas pertinentes, como las organizaciones europeas de normalización, las autoridades nacionales pertinentes, las organizaciones basadas en acuerdos de reconocimiento mutuo como el acuerdo de reconocimiento mutuo del SOG-IS, las pymes, las organizaciones de consumidores y los interlocutores sociales y medioambientales.

(56 *quinquies*) ENISA debe encargarse del mantenimiento de un sitio web que facilite información y publicidad sobre los regímenes europeos de certificación de la ciberseguridad, que debe incluir, entre otras cosas, las solicitudes para preparar una propuesta de régimen europeo de certificación de la ciberseguridad y los comentarios recibidos en el proceso de consulta llevado a cabo por ENISA en la fase de preparación. Dicho sitio web también debe proporcionar información sobre los certificados y las declaraciones de conformidad de la UE expedidos en virtud del presente Reglamento.

(57) El recurso a la certificación europea de la ciberseguridad **y a la declaración de conformidad de la UE** debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación de la Unión o en la legislación nacional **adoptada con arreglo al Derecho de la Unión. Puesto que la legislación no está armonizada, los Estados miembros podrán adoptar reglamentos técnicos nacionales de conformidad con la Directiva (UE) 2015/1535 que establece la certificación obligatoria en el marco de un régimen europeo de certificación de la ciberseguridad. Los Estados miembros también podrían recurrir a la certificación europea de la ciberseguridad en el contexto de la contratación pública y de la Directiva 2014/214/UE**.[…]

(57 *bis*) 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. No obstante, no debe impedirse a los Estados miembros adoptar o conservar regímenes de certificación nacional con fines de seguridad nacional.

(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 **restringir, suspender o** 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) […] Los Estados miembros **[…] deben** designar a una **o más autoridades** […] de certificación de la ciberseguridad para supervisar el cumplimiento **de las obligaciones derivadas del presente Reglamento. Si un Estado miembro lo considera adecuado, las tareas también podrán asignarse a autoridades que ya existen. Asimismo, los Estados miembros deben poder decidir, por mutuo acuerdo con otro Estado miembro, designar a una o más autoridades de supervisión en el territorio de ese otro Estado miembro. En particular, la autoridad debe supervisar y hacer cumplir las obligaciones de los fabricantes o proveedores de productos y servicios de TIC establecidos en sus territorios respectivos en relación con la declaración de conformidad de la UE, asistir a los organismos de acreditación nacionales en el proceso de seguimiento y supervisión de las actividades de los organismos de evaluación de la conformidad facilitándoles conocimientos especializados e información pertinente, autorizar a los organismos de evaluación de la conformidad a desempeñar sus funciones cuando cumplen los requisitos adicionales establecidos en un régimen y supervisar la evolución pertinente en el ámbito de la certificación de la ciberseguridad** […]. Las autoridades nacionales de […] certificación **de la ciberseguridad** deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos **por ellas o por los organismos de evaluación de la conformidad que se refieren al nivel de garantía elevado** […], 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 certificación **de la ciberseguridad** 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 la 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 **representantes de** las autoridades nacionales […] de certificación **de la ciberseguridad u otras autoridades nacionales pertinentes**. 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 Agencia sobre propuestas de regímenes y** a la Comisión relativos al mantenimiento y revisión de los regímenes europeos de certificación de la ciberseguridad existentes.

(60 *bis*) El Grupo debe facilitar el intercambio de buenas prácticas y conocimientos especializados entre las autoridades nacionales de certificación de la ciberseguridad responsables de la autorización de los organismos de evaluación de la conformidad y la expedición de certificados. El Grupo debe apoyar el desarrollo de un mecanismo de revisión interpares en el contexto de la preparación de una propuesta de régimen y su aplicación para los organismos que expidan certificados europeos de ciberseguridad para un nivel de garantía elevado. Dichas revisiones interpares deben evaluar concretamente si los organismos de que se trate tienen los conocimientos especializados adecuados y desempeñan sus funciones de forma armonizada. Los resultados de las revisiones interpares deben hacerse públicos. Estos organismos pueden adoptar las medidas apropiadas para adaptar sus prácticas y sus conocimientos especializados.

(61) Con el fin de reforzar la sensibilización y facilitar la aceptación de los futuros regímenes de ciberseguridad de la UE, la Comisión Europea puede 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.

(61 *bis*) Con el fin de seguir facilitando el comercio y reconociendo que las cadenas de suministro de TIC son mundiales, la Unión, de conformidad con el artículo 218 del TFUE, puede celebrar acuerdos de reconocimiento mutuo relativos a certificados expedidos por regímenes creados con arreglo al marco europeo de certificación de la ciberseguridad. La Comisión, teniendo en cuenta el asesoramiento de ENISA y del Grupo Europeo de Certificación de la Ciberseguridad, puede recomendar que se inicien las negociaciones correspondientes. Cada régimen debe proporcionar condiciones específicas para el reconocimiento mutuo con terceros países.

(62) […]

(63) […]

(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 certificación **de la ciberseguridad**.

(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

1. 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 la Unión Europea para la Ciberseguridad**», 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 **procesos,** 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.

2. **El presente Reglamento se entenderá 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 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 **dañar, perturbar o afectar desfavorablemente de otra manera** 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 **o evaluación de conformidad** de los **procesos,** productos y servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico;

9 *bis*) «régimen nacional de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos desarrollados y adoptados por una autoridad pública nacional aplicables a la certificación o la evaluación de conformidad de los procesos, 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 […] que certifica que determinado **proceso**, producto o servicio de TIC […] **ha sido evaluado para verificar que cumple** los requisitos específicos **de seguridad** establecidos en un régimen europeo de certificación de la ciberseguridad;

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

11 *bis*) «servicio de TIC», cualquier servicio que consista, en su totalidad o principalmente, en la transmisión, almacenamiento, extracción o tratamiento de información mediante redes y sistemas de información;

11 *ter*) «proceso de TIC», todo conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio de TIC;

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**;**

16 *bis*) «especificaciones técnicas», un documento que prescribe los requisitos técnicos que debe cumplir un proceso, producto o servicio de TIC;

16 *ter*) «nivel de garantía», motivo para confiar en que un proceso, producto o servicio de TIC cumple los requisitos de seguridad de un régimen europeo específico de certificación de la ciberseguridad y establece el nivel en el que se ha evaluado; el nivel de garantía no mide la seguridad de un proceso, producto o servicio de TIC en sí mismo.

TÍTULO II

ENISA, la «*Agencia […] de la Unión Europea para la ciberseguridad*»

CAPÍTULO I

MANDATO Y OBJETIVOS*[…]*

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 […] **en toda** la Unión, **especialmente mediante el apoyo a los Estados miembros y a las instituciones, los órganos y los organismos de la Unión en la mejora de la ciberseguridad**. **La Agencia actuará como punto de referencia de asesoramiento y conocimientos en cuestiones relacionadas con la ciberseguridad para las instituciones, los órganos y los organismos 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.

2 *bis*. Al desempeñar sus funciones, la Agencia actuará con independencia y tendrá debidamente en cuenta los conocimientos nacionales de las autoridades pertinentes de los Estados miembros, evitando al mismo tiempo la duplicación de actividades.

3. […]

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 **de la Unión** relativas a la ciberseguridad**, en particular políticas sectoriales sobre ciberseguridad**.

3. La Agencia prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a **las instituciones, órganos y organismos de esta**, **así como a** los Estados miembros y las partes interesadas públicas y privadas a fin de incrementar la protección de sus redes y sistemas de información, desarrollar **y mejorar la ciberresiliencia y la capacidad de respuesta y desarrollar** las capacidades y competencias en el ámbito de la ciberseguridad […].

4. La Agencia fomentará la cooperación y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, **públicas y privadas** […], sobre las cuestiones relacionadas con la ciberseguridad.

5. La Agencia **contribuirá a incrementar** […] las capacidades de ciberseguridad a nivel de la Unión para […] **prestar asistencia** a 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, **con vistas a evitar la fragmentación de los regímenes de certificación en la UE**. **En particular, la Agencia contribuirá** […] a la creación y al 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.

CAPÍTULO I BIS

FUNCIONES

Artículo 5

[…] ***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. Respaldando:

   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. Respaldando 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 […] **incidentes** relacionados con 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

[...] ***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 […] **ciberamenazas** […] 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 […] **ciberamenazas** […] e incidentes de ciberseguridad, **en particular** 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 […] **seguirá** 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 ejercicios **regulares** de ciberseguridad […] 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 **en** […] 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 **apoyará la puesta en común de información dentro de los sectores y entre ellos** […], 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

[...] ***Cooperación operativa a nivel de la Unión***

1. La Agencia apoyará la cooperación operativa entre **los Estados miembros, las instituciones, los órganos y** los organismos de la Unión […] 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 **como tal** facilitará […] el intercambio de información y la cooperación entre sus miembros.

4. La Agencia **apoyará** […] la cooperación operativa dentro de la red de CSIRT y prestará apoyo a los Estados miembros**, a instancia de estos**:

a) asesorando sobre cómo mejorar su capacidad para prevenir, detectar y dar respuesta a los incidentes;

b) […] **facilitando la gestión** técnica […] de incidentes con un impacto significativo o sustancial, **en particular apoyando el intercambio voluntario de soluciones técnicas entre Estados miembros**;

c) analizando las vulnerabilidades […] e incidentes**;**

c *bis*) dando apoyo en las investigaciones técnicas ex post de los incidentes que tengan un impacto significativo o sustancial con arreglo a la Directiva (UE) 2016/1148.

En el desempeño de estas funciones, la Agencia y el CERT-UE entablarán una cooperación estructurada con el fin de beneficiarse de las sinergias **y evitar la duplicación de actividades** […].

5. […]

[…]

6. La Agencia organizará […] **regularmente** 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. **Dichos ejercicios a nivel de la Unión podrán constar de elementos técnicos, operativos o estratégicos** […]. **Cada dos años, se organizará un ejercicio a gran escala que tendrá todos esos elementos.** La Agencia participará asimismo en la realización de ejercicios sectoriales de ciberseguridad, y contribuirá a organizarlos cuando proceda, junto con […] **organizaciones pertinentes que puedan** participar también en los ejercicios de ciberseguridad a nivel de la Unión.

7. La Agencia**, en estrecha colaboración con los Estados miembros,** 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 […] o los puntos de contacto únicos de la Directiva SRI (**ambos con carácter voluntario** […]); 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 **puestos en común de manera voluntaria**, 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) […] **a petición de los Estados miembros, facilitación** de la gestión técnica de un incidente o crisis, **en particular […] apoyando** la puesta en común **voluntaria** de soluciones técnicas entre los Estados miembros;

d) apoyo a **las instituciones, órganos y organismos de la UE y, previa petición, a los Estados miembros en** la comunicación pública en torno al incidente o crisis;

e) **apoyo a los Estados miembros, a instancia de estos, para probar** […] los planes de cooperación para responder a estos incidentes o crisis.

Artículo 8

*[...] **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 **procesos,** 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 **procesos**, productos y servicios de TIC **en cooperación con la industria y** 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 certificación **de la ciberseguridad** y con la industria.

3 *bis*) recomendar unas especificaciones técnicas apropiadas que se puedan utilizar en el desarrollo de los regímenes europeos de certificación de la ciberseguridad mencionados en el artículo 47, apartado 1, letra b), cuando no se disponga de normas;

3 *ter*) contribuir a una creación de capacidades suficiente relacionada con los procesos de evaluación y certificación, recopilando y publicando directrices y proporcionando apoyo a los Estados miembros, a instancia de estos;

b) facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los **procesos**, productos y servicios de TIC […]**;**

b *bis*) 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

[...] ***Conocimiento* e *información*** […]

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 […] **incidentes de** 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 las infraestructuras que sustentan los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148 **y las utilizadas por los proveedores de servicios digitales enumerados en el anexo III de dicha Directiva**;

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 **y, de manera voluntaria, por los Estados miembros y las partes interesadas públicas y privadas**;

e) […]

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) […].

Artículo 9 **bis**

Sensibilización y educación

La Agencia:

a) sensibilizará al público sobre los riesgos relacionados con la ciberseguridad y facilitará orientaciones sobre buenas prácticas para usuarios individuales, dirigidas a ciudadanos y organizaciones;

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

c) asistirá a los Estados miembros en sus esfuerzos para sensibilizar sobre la ciberseguridad y promover la formación en este ámbito;

d) apoyará una mejor coordinación y el intercambio de mejores prácticas entre Estados miembros sobre educación y sensibilización en materia de ciberseguridad, facilitando la creación y el mantenimiento de una red de puntos de contacto educativos nacionales.

Artículo 10

[...] ***Investigación e 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

[...] ***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, […] **dentro de los marcos de cooperación internacional pertinentes**, el intercambio de mejores prácticas […];

c) facilitar asesoramiento a la Comisión cuando así se solicite**;**

c *bis*) facilitar, en colaboración con el Grupo Europeo de Certificación de la Ciberseguridad creado en virtud del artículo 53, asesoramiento y apoyo a la Comisión en materia de acuerdos de reconocimiento mutuo de certificados de ciberseguridad con terceros países.

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; […]

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

d *bis*) una red de funcionarios de enlace nacionales, que ejercerá las funciones definidas en el artículo 20 *bis*.

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;

c *bis*) supervisará la aplicación de la programación anual y plurianual que figura en el documento único de programación;

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. […]

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, **en particular la aplicación del programa de trabajo anual**, 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;

l *bis*) intercambiar regularmente con las instituciones, órganos y organismos de la Unión información sobre sus actividades en materia de ciberseguridad para garantizar la coherencia en el desarrollo y la aplicación de la política de la UE;

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. **Cuando sea necesario, con el fin de desempeñar las funciones de la Agencia de manera eficiente y eficaz y sobre la base de un análisis adecuado de los costes y los beneficios, el** director ejecutivo **podrá** decidir […] **establecer una o más oficinas locales en uno o más Estados miembros**. Antes de tomar la decisión de establecer una oficina local, el director ejecutivo **pedirá la opinión del Estado o Estados miembros afectados, en particular del Estado miembros donde se encuentra la sede de la Agencia, y** habrá de obtener el consentimiento previo de la Comisión **y** del Consejo de Administración […]. **En caso de desacuerdo durante el proceso de consulta entre el director ejecutivo y los Estados miembros afectados, el asunto será debatido en el Consejo.** La decisión especificará el alcance de las actividades que se llevarán a cabo en la oficina local, evitándose costes innecesarios y duplicación de funciones administrativas de la Agencia. […] **El número de efectivos en todas las oficinas locales se mantendrá en un mínimo y no superará en total el 40 % del […] personal ubicado en el Estado miembro donde se encuentra la sede de la Agencia. El número de efectivos en cada oficina local no superará el 10 % del […] personal ubicado en el Estado miembro donde se encuentra la sede de la Agencia.**

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 operadores de servicios esenciales,** 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.

5 *bis*. El Grupo Permanente de Partes Interesadas informará regularmente al Consejo de Administración de sus actividades.

SECCIÓN 4 *BIS*

RED DE FUNCIONARIOS DE ENLACE NACIONALES

Artículo 20 bis

Red de funcionarios de enlace nacionales

1. El Consejo de Administración, a propuesta del director ejecutivo, establecerá una red de funcionarios de enlace nacionales, formada por representantes de los Estados miembros.

2. La red de funcionarios de enlace nacionales estará formada por representantes de todos los Estados miembros. Cada Estado miembro nombrará a un representante. Las reuniones de la red se celebrarán en distintos formatos de expertos.

3. En particular, la red de funcionarios de enlace nacionales facilitará el intercambio de información entre ENISA y los Estados miembros. Apoyará especialmente a ENISA en la difusión de sus actividades, conclusiones y recomendaciones a las partes interesadas pertinentes en toda la UE.

4. Los funcionarios de enlace nacionales actuarán como puntos centrales de contacto a nivel nacional para facilitar la cooperación entre ENISA y los expertos nacionales en el contexto de la aplicación del programa de trabajo de ENISA.

5. Aunque los funcionarios de enlace nacionales trabajarán en estrecha cooperación con los representantes del Consejo de Administración en sus respectivos países, la red en sí misma no duplicará el trabajo del Consejo de Administración ni de otros foros de la UE.

6. Las funciones y los procedimientos de la red de funcionarios de enlace nacionales estarán especificados en el reglamento operativo interno de la Agencia y serán públicos.

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 Comisión[14] 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.

[14] 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).

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. 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) 2015/443[15] y 2015/444[16] de la Comisión. Dicho reglamento incluirá, entre otras, disposiciones para el intercambio, tratamiento y almacenamiento de la información clasificada.

---

15 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).

16 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).

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.

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 Consejo[17], 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.

---

[17] 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).

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 n.º 883/2013 del Parlamento Europeo y del Consejo y el Reglamento (Euratom, CE) n.º 2185/96 del Consejo[18], 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.

---

18 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 **cuatro** […] 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 **cuatro** […] 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 destituido por decisión del Consejo de Administración […].

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 **bien** vender propiedad mobiliaria e inmobiliaria y ser parte en actuaciones judiciales.

3. La Agencia estará representada por su director ejecutivo.

Artículo 36

Responsabilidad civil 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 1[19]. 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.

Artículo 38

Protección de los datos de carácter personal

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 Consejo[20].

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.

---

[19] 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).

[20] 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 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.

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 […] condiciones […] 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

Marco *europeo de certificación de la ciberseguridad* […]

1. **Se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión. Establece una gobernanza que permite un enfoque armonizado a nivel de la UE de los regímenes europeos de certificación de la ciberseguridad, al objeto de la creación de un mercado único digital para los procesos, productos y servicios de TIC.**

2. **El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar regímenes** […] europeos de certificación de la ciberseguridad […] **y a confirmar** que los **procesos**, productos y servicios de TIC que hayan sido […] **evaluados** con arreglo a dichos **regímenes** cumplen los requisitos **de seguridad** especificados […] **con el objetivo de proteger** 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 **y** servicios […] **durante todo su ciclo de vida**.

Artículo 44

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

1. Tras recibir una solicitud de la Comisión **o del Grupo Europeo de Certificación de la Ciberseguridad (el «Grupo») creado en virtud del artículo 53**, 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.[…]

1 *bis*. Los Estados miembros u organizaciones de partes interesadas podrán proponer al Grupo la preparación de una propuesta de régimen europeo de certificación de la ciberseguridad. El Grupo evaluará las propuestas atendiendo a unos criterios definidos por el Grupo mediante directrices con arreglo al artículo 53, apartado 3, letra c *bis*), y podrá solicitar a ENISA que prepare una propuesta de 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 **mediante procesos de consulta transparentes** y cooperará estrechamente con el Grupo. El Grupo facilitará a ENISA la asistencia y el asesoramiento experto […] en relación con la preparación de la propuesta de régimen **y adoptará un dictamen sobre la propuesta de régimen antes de su presentación a la Comisión.** […]. **ENISA velará por que las propuestas de régimen sean coherentes con la norma armonizada aplicable utilizada para la acreditación del órgano de evaluación de la conformidad.**

3. ENISA **tomará en máxima consideración el dictamen del Grupo antes de transmitir a la Comisión** la propuesta de régimen […] 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 2, que establezcan regímenes europeos de certificación de la ciberseguridad para **procesos,** productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento.

5. […]

Artículo 44 bis

Mantenimiento del régimen europeo de certificación de la ciberseguridad

1. La Agencia mantendrá un sitio web asignado a este propósito en el que se facilite información sobre los regímenes europeos de certificación de la ciberseguridad, los certificados y las declaraciones de conformidad de la UE emitidos con arreglo al artículo 47 *bis* y se les dé publicidad.

2. La Agencia, en estrecha cooperación con el Grupo, revisará al menos cada cinco años los regímenes europeos de certificación de la ciberseguridad teniendo en cuenta los comentarios recibidos de las partes interesadas. Si lo considera necesario, la Comisión o el Grupo podrán pedir a la Agencia que dé inicio al proceso de desarrollo de una propuesta revisada de régimen con arreglo al artículo 44, apartados 2 y 3.

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 […] **cumplir**, según proceda, **al menos** 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 **durante todo el ciclo de vida del proceso, producto o servicio**;

b) proteger los datos almacenados, transmitidos o procesados de otro modo frente a la destrucción accidental o no autorizada, la pérdida […] o la alteración **durante todo el ciclo de vida del proceso, producto o servicio**;

c) […] 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 […] **sido objeto de acceso, de uso o de otro procesamiento**, en qué momentos y por quién;

e) […] que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso**,** […] de uso **o de otro procesamiento**, 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) […] que los **procesos,** productos y servicios de TIC se entreguen siempre con un software **y un hardware** actualizados, que no contenga**n** vulnerabilidades conocidas **públicamente**, y dispongan de mecanismos para efectuar actualizaciones de seguridad […]**;**

g *bis*) que los procesos, productos y servicios de TIC se desarrollen, fabriquen y suministren con arreglo a los requisitos de seguridad que figuren en el régimen en cuestión.

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 **procesos,** productos y servicios de TIC […].**El nivel de garantía deberá ser proporcional al nivel de riesgo asociado con el uso previsto de un proceso, producto o servicio de TIC.**

2. Los niveles de garantía básico, sustancial y elevado […] **se referirán a un certificado o a una declaración de conformidad de la UE expedidos en el contexto de un régimen europeo de certificación de la ciberseguridad que determina para cada nivel de garantía los requisitos de seguridad respectivos, incluidas las funcionalidades de seguridad y el grado de dedicación necesario para evaluar un proceso, producto o servicio de TIC. El certificado o la declaración de conformidad de la UE se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es reducir el riesgo de incidentes de ciberseguridad o evitarlos de la forma siguiente:**

a) **un certificado europeo de ciberseguridad o una declaración de conformidad de la UE que se refiere a un** nivel de garantía «básico» **ofrece garantías de que los procesos, productos y servicios de TIC cumplen los respectivos requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos básicos conocidos de ciberincidentes y ciberataques. Las actividades de evaluación incluirán al menos una revisión de la documentación técnica o, cuando no proceda, incluirán actividades de sustitución con efecto equivalente** […];

b) **un certificado europeo de ciberseguridad que se refiere a un** nivel de garantía «sustancial» **ofrece garantías de que los procesos, productos y servicios de TIC cumplen los respectivos requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos básicos conocidos de ciberriesgos, ciberincidentes y ciberataques cometidos por agentes con capacidades y recursos limitados. Las actividades de evaluación incluirán al menos: la revisión de la improcedencia de las vulnerabilidades conocidas públicamente y la comprobación de que los procesos, productos o servicios de TIC aplican correctamente la necesaria funcionalidad de seguridad; o, cuando no proceda, incluirán actividades de sustitución con efecto equivalente**[…];

c) **un certificado europeo de ciberseguridad que se refiere a un** nivel de garantía «elevado» **ofrece garantías de que los procesos, productos y servicios de TIC cumplen los respectivos requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables. Las actividades de evaluación incluirán al menos: la revisión de la improcedencia de las vulnerabilidades conocidas públicamente, la comprobación de que los procesos, productos o servicios de TIC aplican correctamente la necesaria funcionalidad de seguridad, con las tecnologías más avanzadas, y la evaluación de su resistencia a atacantes expertos mediante tests de intrusión; o, cuando no proceda, incluirán actividades de sustitución con efecto equivalente**[…].

2 *bis*. Un régimen europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y la profundidad de la metodología de evaluación. Cada uno de los niveles de evaluación corresponderá a uno de los niveles de garantía y estará definido por una combinación apropiada de componentes de garantía.

Artículo 47

Elementos de los regímenes europeos de certificación de la ciberseguridad

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

a) objeto y alcance **del régimen** de certificación, incluido el tipo o categoría de **procesos**, productos y servicios de TIC cubiertos, **así como una explicación del modo en que el régimen de certificación satisface las necesidades de los grupos destinatarios esperados**;

b) […] referencia a las normas […] internacionales, **europeas o nacionales que se han seguido para hacer la evaluación. En caso de que no haya normas disponibles, se deberá hacer referencia a las** […] especificaciones técnicas **que cumplen los requisitos del anexo II del Reglamento 1025/2012 o, si no estuvieran disponibles, a las especificaciones técnicas o a otros requisitos de seguridad definidos en el régimen**;

c) en su caso, uno o varios niveles de garantía;

c *bis*) en su caso, requisitos específicos o adicionales aplicables a los organismos de evaluación de la conformidad a fin de garantizar su capacidad técnica para evaluar los requisitos en materia de ciberseguridad;

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) **en su caso,** información necesaria para la certificación que deben facilitar **o poner a disposición de otro modo** 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) […] normas para controlar el cumplimiento de los requisitos de los certificados **o de la declaración de conformidad de la UE**, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

h) **en su caso,** condiciones para la concesión **y renovación de un certificado**, **así como para** el mantenimiento, la continuación, la ampliación **o** 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 **o autoevaluados** con los requisitos […] **del régimen**;

j) normas sobre cómo deben notificarse y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en **procesos**, productos y servicios de TIC;

k) **en su caso,** normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad;

l) identificación de los regímenes nacionales **o internacionales** de certificación de la ciberseguridad que cubren el mismo tipo o categoría de **procesos,** productos y servicios de TIC, **requisitos de seguridad y criterios y métodos de evaluación;**

m) contenido del certificado expedido **o declaración de conformidad de la UE;**

m *bis*) el periodo de almacenamiento de la declaración de conformidad de la UE y la documentación técnica de toda la información pertinente proporcionada por el fabricante o el proveedor de productos y servicios de TIC;

m *ter*[…]) periodo máximo de validez de los certificados;

m *quater*[…]) política de divulgación para certificados concedidos, modificados o retirados;

m *quinquies*[…]) condiciones para el reconocimiento mutuo de regímenes de certificación de terceros países;

m *sexies*[…]) en su caso, normas relativas a un mecanismo de revisión interpares para los organismos que expidan certificados europeos de ciberseguridad para un nivel de garantía elevado […] con arreglo al artículo 48, apartado 4 *bis*.

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 **o la declaración de conformidad de la UE** 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 47 bis

Autoevaluación de la conformidad

1. Un régimen europeo de certificación de la ciberseguridad podrá permitir realizar una evaluación de la conformidad bajo la responsabilidad exclusiva del fabricante o proveedor de productos y servicios de TIC. Dicha evaluación de la conformidad será aplicable únicamente a productos y servicios de TIC de bajo riesgo correspondientes al nivel de garantía básico.

2. El fabricante o el proveedor de los productos y servicios de TIC puede expedir una declaración de conformidad de la UE donde declare que queda demostrado el cumplimiento de los requisitos establecidos por el régimen. Al establecer dicha declaración, el fabricante o proveedor de productos y servicios de TIC asumirá la responsabilidad de la conformidad del producto o servicio de TIC con los requisitos que establezca el régimen.

3. El fabricante o proveedor de productos y servicios de TIC deberá poner a disposición de la autoridad nacional de certificación de la seguridad a que se refiere el artículo 50, apartado 1, la declaración de conformidad de la UE y la documentación técnica de toda la información pertinente relativa a la conformidad de los productos o servicios de TIC con un régimen durante un plazo definido en el régimen europeo de certificación de la ciberseguridad correspondiente. Deberá presentarse a la autoridad nacional de supervisión de la certificación y a ENISA una copia de la declaración de conformidad de la UE.

4. La expedición de la declaración de conformidad de la UE será voluntaria, a menos que el Derecho de la Unión o de los Estados miembros especifique lo contrario.

5. La declaración de conformidad de la UE expedida de conformidad con el presente artículo será reconocida en todos los Estados miembros.

Artículo 48

Certificación de la ciberseguridad

1. Los **procesos**, 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 **o de los Estados miembros**.

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 **que haga referencia al nivel de garantía básico o sustancial**, 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 **certificación de la** ciberseguridad particular podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese régimen. Este organismo […] será uno de los siguientes:

a) una autoridad nacional de […] certificación **de la ciberseguridad** con arreglo al artículo 50, apartado 1;

b) un organismo **público** que esté acreditado como organismo de evaluación de la conformidad con arreglo al artículo 51, apartado 1; […]

c) […].

4 *bis*) En los casos en que un régimen europeo de certificación de la ciberseguridad en virtud del artículo 44 requiera un nivel de garantía elevado, el certificado solo podrá ser expedido por una autoridad nacional de certificación de la ciberseguridad contemplada en el artículo 50, apartado 1, o por un organismo de evaluación de la conformidad contemplado en el artículo 51, en las siguientes condiciones:

a) previa aprobación de la autoridad nacional de certificación de la ciberseguridad para cada certificado individual que expida un organismo de evaluación de la conformidad; o

b) previa delegación general de esta misión de la autoridad nacional de certificación de la ciberseguridad en un organismo de evaluación de la conformidad.

5. La persona física o jurídica que presenta sus **procesos**, productos o servicios de TIC al mecanismo de certificación […] **pondrá a disposición del** organismo de evaluación de la conformidad a que se refiere el artículo 51 **o la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 50, si dicha autoridad es el organismo que expide el certificado,** […] toda la información necesaria para llevar a cabo el procedimiento de certificación.

5 *bis*. El titular de un certificado informará al organismo que expidió dicho certificado de cualquier vulnerabilidad o irregularidad que detecte posteriormente, relativa a la seguridad de los procesos, productos o servicios de TIC, que pueda afectar a los requisitos de certificación. El organismo transmitirá dicha información sin demora indebida a la autoridad nacional de certificación de la ciberseguridad.

6. Los certificados se expedirán por […] **el período definido en el régimen particular de certificación** y podrán renovarse […] 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 **procesos,** 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 y los procedimientos conexos para los **procesos,** 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 **procesos,** 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 **y cubiertos por un régimen europeo de certificación de la ciberseguridad** seguirán siendo válidos hasta su fecha de caducidad.

Artículo 50

***Autoridades nacionales de**[...] **certificación* de la ciberseguridad**

1. Cada Estado miembro **designará a una o más autoridades** nacionales de […] certificación de la **ciberseguridad en su territorio o, de mutuo acuerdo con otro Estado miembro, designará a una o más autoridades establecidas en ese otro Estado miembro para que sean responsables de las tareas de supervisión en el Estado miembro que efectúe la designación.**

2. Cada Estado miembro informará a la Comisión de la identidad de **las autoridades designadas y de las tareas que se les hayan encomendado**.

3. **Sin perjuicio de lo establecido en el artículo 48, apartado 4, letra a), y en el artículo 48, apartado 4 *bis*,** las autoridades nacionales de […] certificación **de la ciberseguridad** 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.

3 *bis*. Los Estados miembros se asegurarán de que las actividades de la autoridad nacional de certificación de la ciberseguridad relacionadas con la expedición de certificados de conformidad con el artículo 48, apartado 4, letra a) y el artículo 48, apartado 4 bis, se acogen a una estricta separación de funciones y responsabilidades con respecto a las actividades de supervisión del presente artículo y que ambas actividades funcionan de manera independiente.

4. Los Estados miembros velarán por que las autoridades nacionales de […] certificación **de la ciberseguridad** 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 […] certificación **de la ciberseguridad**:

a) […]

a *bis*) controlarán y velarán por la aplicación de las obligaciones del fabricante o proveedor de productos y servicios de TIC establecidos en sus respectivos territorios, que figuran en el artículo 47 *bis*, apartados 2 y 3, y en los correspondientes regímenes europeos de certificación de la ciberseguridad;

b) […] **sin perjuicio de lo dispuesto en el artículo 51, apartado 1 *ter*, asistirán a los organismos nacionales de acreditación en el control y la supervisión de** las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento […];

b *bis*) controlarán y supervisarán las actividades de los organismos mencionados en el artículo 48, apartado 4;

b *ter*) autorizarán a los organismos de evaluación de la conformidad mencionados en el artículo 51, apartado 1 *ter*, y restringirán, suspenderán o retirarán las autorizaciones en vigor en caso de incumplimiento de los requisitos del presente Reglamento;

c) tramitarán las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por […] **las autoridades nacionales de certificación de la ciberseguridad o, de conformidad con el artículo 48, apartado 4 *bis*, por los organismos de evaluación de la conformidad**, 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 […] certificación **de la ciberseguridad** u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles **procesos,** 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 […] certificación **de la ciberseguridad** tendrá, como mínimo, las siguientes competencias:

a) solicitar a los organismos de evaluación de la conformidad**,** […] a los titulares de certificados europeos de ciberseguridad **y a los responsables de expedir declaraciones de conformidad de la UE** 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**,** […] los titulares de certificados europeos de ciberseguridad **y los responsables de expedir declaraciones de conformidad de la UE**, 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**,** […] los titulares de certificados **y los responsables de expedir declaraciones de conformidad de la UE** 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 **emitidos por la autoridad nacional de certificación de la ciberseguridad o, de conformidad con el artículo 48, apartado 4 *bis*, por los organismos de evaluación de la conformidad** 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 […] certificación **de la ciberseguridad** 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 **procesos,** 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.

1 *bis*. Cuando una autoridad nacional de certificación de la ciberseguridad expida un certificado europeo de ciberseguridad de conformidad con el artículo 48, apartado 4, letra a), y apartado 4 *bis*, el organismo de certificación de la autoridad nacional de certificación de la ciberseguridad será acreditado como organismo de evaluación de la conformidad con arreglo al apartado 1 del presente artículo.

1 *ter*. En su caso, los organismos de evaluación de la conformidad estarán autorizados por la autoridad nacional de certificación de la ciberseguridad a llevar a cabo sus tareas cuando cumplan requisitos específicos o adicionales establecidos en el régimen de certificación europeo con arreglo al artículo 47, apartado 1, letra c *bis*).

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 **tomarán todas las medidas necesarias dentro de un periodo razonable de tiempo para restringir, suspender o revocar** 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 […] certificación **de la ciberseguridad** notificarán a la Comisión los correspondientes organismos de evaluación de la conformidad acreditados **y, en su caso, autorizados de conformidad con el artículo 51, apartado 1 *ter***, 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 […] certificación **de la ciberseguridad** 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 dicho Estado miembro. 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 […] certificación **de la ciberseguridad**.

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 **representantes de** las autoridades nacionales de […] certificación **de la ciberseguridad o por representantes de otras autoridades nacionales pertinentes**. […] **Cualquier miembro del Grupo solo podrá representar a otro Estado miembro**.

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;

b *bis*) adoptar un dictamen sobre la propuesta de régimen, de conformidad con el artículo 44 del presente Reglamento;

c) […] **solicitar** a la Agencia que prepare una propuesta de régimen europeo de certificación de la ciberseguridad de conformidad con el artículo 44 del presente Reglamento;

c *bis*) desarrollar y adoptar directrices sobre los criterios de evaluación de las propuestas para la preparación de una propuesta de régimen presentada […] al Grupo de conformidad con el artículo 44, apartado 1 *bis*;

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 […] certificación **de la ciberseguridad** en virtud del presente título mediante **creación de capacidades,** 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**;**

f *bis*) proporcionar apoyo a la aplicación del mecanismo de revisión interpares según las normas establecidas en un régimen europeo de certificación de la ciberseguridad de conformidad con lo dispuesto en el artículo 47, apartado 1, letra m *quinquies*), del presente Reglamento.

4. La Comisión presidirá el Grupo **en calidad de moderador** y se hará cargo de su secretaría, con la asistencia de ENISA según lo previsto en el artículo 8, letra a).

***Artículo 53* bis**

***Derecho a presentar una reclamación ante la autoridad nacional de […] certificación* de la ciberseguridad**

1. Las personas físicas o jurídicas tendrán derecho a presentar una reclamación ante la autoridad nacional de certificación de la ciberseguridad relativa a un certificado expedido por esa misma autoridad o, de conformidad con el artículo 48, apartado 4 *bis*, por los organismos de evaluación de la conformidad.

2. La autoridad nacional de certificación de la ciberseguridad ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 53 *ter*.

Artículo 53 **ter**

Derecho a la tutela judicial efectiva

1. Las personas físicas o jurídicas tendrán derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante que les afecte, tomada por una autoridad nacional de certificación de la ciberseguridad.

2. Las personas físicas o jurídicas tendrán derecho a la tutela judicial efectiva en caso de que la autoridad nacional de certificación de la ciberseguridad no tramite una reclamación.

3. Los procesos contra una autoridad nacional de certificación de la ciberseguridad se dirimirán en los tribunales del Estado miembro donde esté establecida la autoridad.

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 5**, apartado 4, letra b)**, 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

Entrada en vigor

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

1 *bis*. El presente Reglamento se aplicará a partir de […], excepto los artículos 50, 51, 52, 53 *bis*, 53 *ter* y 54, que se aplicarán a partir de [24 meses después de la fecha 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	*Por el Consejo*
El Presidente	*El Presidente*

ANEXO

REQUISITOS QUE DEBEN CUMPLIR LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD

Los organismos de evaluación de la conformidad que deseen ser acreditados deberán cumplir los siguientes requisitos:

1. El organismo de evaluación de la conformidad se establecerá de conformidad con el Derecho interno y tendrá personalidad jurídica.

2. El organismo de evaluación de la conformidad será un organismo tercero independiente de la organización o de los productos y servicios de TIC que evalúa.

3. Podrá tratarse de un organismo perteneciente a una asociación empresarial o una federación profesional que represente a las empresas que participan en el diseño, la fabricación, el suministro, el montaje, el uso o el mantenimiento de los productos o servicios de TIC que evalúa, a condición de que se demuestre su independencia y la ausencia de conflictos de intereses.

4. El organismo de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no serán el diseñador, el fabricante, el proveedor, el instalador, el comprador, el propietario, el usuario ni el encargado del mantenimiento del producto o servicio de TIC que debe evaluarse, ni tampoco el representante autorizado de ninguno de ellos. Ello no será óbice para que se utilicen los productos evaluados necesarios para las actividades del organismo de evaluación de la conformidad o para que se utilicen dichos productos para fines personales.

5. El organismo de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, la fabricación o construcción, la comercialización, la instalación, el uso o el mantenimiento de los productos o servicios de TIC, ni representarán a las partes que participan en estas actividades. No efectuarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que estén notificados. Ello se aplicará, en particular, a los servicios de consultoría.

6. Los organismos de evaluación de la conformidad se asegurarán de que las actividades de sus filiales o subcontratistas no afecten a la confidencialidad, objetividad o imparcialidad de sus actividades de evaluación de la conformidad.

7. Los organismos de evaluación de la conformidad y su personal llevarán a cabo las actividades de evaluación de la conformidad con el máximo nivel de integridad profesional y con la competencia técnica exigida para el campo específico y serán ajenos a cualquier presión o incentivo, incluidos los de índole financiera, que pueda influir en su apreciación o en los resultados de sus actividades de evaluación de la conformidad, en particular por lo que respecta a personas o grupos de personas que tengan algún interés en los resultados de esas actividades.

8. El organismo de evaluación de la conformidad deberá ser capaz de llevar a cabo todas las tareas de evaluación de la conformidad que le hayan sido asignadas en virtud del presente Reglamento, tanto si dichas tareas las efectúa el propio organismo como si se realizan en su nombre y bajo su responsabilidad.

9. En todo momento, respecto a cada procedimiento de evaluación de la conformidad y cada tipo, categoría o subcategoría de producto o servicio de TIC, el organismo de evaluación de la conformidad dispondrá:

a) del personal necesario con conocimientos técnicos y experiencia suficiente y adecuada para realizar las tareas de evaluación de la conformidad;

b) de las descripciones necesarias de los procedimientos con arreglo a los cuales se efectúa la evaluación de la conformidad, garantizando la transparencia y la posibilidad de reproducción de estos procedimientos; dispondrá asimismo de las políticas y procedimientos adecuados que permitan distinguir entre las tareas efectuadas en tanto que organismo notificado y cualquier otra actividad;

c) de los procedimientos necesarios para desempeñar sus actividades teniendo debidamente en cuenta el tamaño de una empresa, el sector en que opera, su estructura, el grado de complejidad de la tecnología del producto o servicio de TIC de que se trate y si el proceso de producción es en serie.

10. El organismo de evaluación de la conformidad dispondrá de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrá acceso a todos los equipos e instalaciones que necesite.

11. El personal que efectúe las actividades de evaluación de la conformidad tendrá:

a) una sólida formación técnica y profesional referida a todas las actividades de evaluación de la conformidad;

b) un conocimiento satisfactorio de los requisitos de las evaluaciones que efectúe y la autoridad apropiada para efectuar tales evaluaciones;

c) un conocimiento y una comprensión adecuados de los requisitos y normas de ensayo aplicables;

d) la capacidad necesaria para elaborar certificados, documentos e informes que demuestren que se han efectuado las evaluaciones.

12. Se garantizará la imparcialidad del organismo de evaluación de la conformidad, de sus máximos directivos y de su personal de evaluación.

13. La remuneración de los máximos directivos y del personal de evaluación del organismo de evaluación de la conformidad no dependerá del número de evaluaciones que efectúe ni de los resultados de dichas evaluaciones.

14. El organismo de evaluación de la conformidad suscribirá un seguro de responsabilidad, salvo que el Estado asuma la responsabilidad con arreglo al Derecho interno, o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

15. El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información obtenida en el marco de las tareas realizadas con arreglo al presente Reglamento o a cualquier disposición de Derecho nacional por la que se aplique, salvo con respecto a las autoridades competentes de los Estados miembros en que realice sus actividades.

16. Los organismos de evaluación de la conformidad cumplirán los requisitos de la norma **pertinente armonizada por el Reglamento (CE) 765/2008 para la acreditación de los organismos de evaluación de la conformidad que certifiquen procesos, productos o servicios**[…].

17. Los organismos de evaluación de la conformidad velarán por que los laboratorios de ensayo utilizados con fines de evaluación de la conformidad cumplan los requisitos de la norma **pertinente armonizada por el Reglamento (CE) 765/2008 para la acreditación de los laboratorios que realicen ensayos** […].