REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la 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 acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Visto el dictamen del Comité de las Regiones ([2]),

De conformidad con el procedimiento legislativo ordinario ([3]),

Considerando lo siguiente:

(1) Las redes y los sistemas de información y las redes y servicios de comunicaciones electrónicas desempeñan un papel vital en la sociedad y se han convertido en la espina dorsal del crecimiento económico. Las tecnologías de la información y la comunicación (TIC) son la base de los complejos sistemas que sustentan las actividades cotidianas de la sociedad, garantizan el funcionamiento de nuestras economías en sectores clave como la salud, la energía, las finanzas y el transporte y, en particular, respaldan el funcionamiento del mercado interior.

(2) La utilización de las redes y los sistemas de información por los ciudadanos, organizaciones y empresas de toda la Unión está ya muy generalizada. La digitalización y la conectividad se están convirtiendo en elementos esenciales de un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera que durante la próxima década se utilicen en la Unión un número extremadamente alto de dispositivos digitales conectados. 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, las organizaciones y las empresas de información suficiente sobre las características de ciberseguridad de los productos de ITC, servicios de TIC y los procesos de ITC, lo que socava la confianza en las soluciones digitales.

(3) La intensificación de la digitalización y de la conectividad trae consigo un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resulta más vulnerable a las ciberamenazas y se exacerban los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar dichos riesgos, es preciso adoptar todas las medidas necesarias para mejorar la ciberseguridad en la Unión a fin de proteger mejor de las ciberamenazas a las redes y los sistemas de información, las redes de telecomunicaciones y los productos, los servicios y dispositivos digitales utilizados por los ciudadanos, las organizaciones y las empresas, desde las pequeñas y medianas empresas (pymes), según se definen en la Recomendación n.º 2003/361/CE ([4]) de la Comisión, a los operadores de infraestructuras críticas.

([1]) DO C 227 de 28.6.2018, p. 86.
([2]) DO C 176 de 23.5.2018, p. 29.
([3]) Posición del Parlamento Europeo de 12 de marzo de 2019 (pendiente de publicación el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.
([4]) Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

(4) Al hacer que la información pertinente esté a disposición del público, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) establecida por el Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo ([5]) contribuye al desarrollo del sector de la ciberseguridad en la Unión, en particular en lo que respecta a las pymes y las empresas emergentes. ENISA debe trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión y reforzar las cadenas de suministro de dentro de la Unión.

(5) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y los ciberataques, requieren unas defensas más sólidas. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las competencias de las autoridades de ciberseguridad y policiales, así como las respuestas políticas de las mismas, son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la Unión. Esta situación requiere una respuesta efectiva y coordinada y una gestión de crisis a escala de la Unión, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad y la asistencia mutua en Europa. Además, es importante para los responsables políticos, la industria y los usuarios que se lleve a cabo una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables de la Unión, y que se haga una previsión sistemática de los avances, retos y amenazas futuros.

(6) A la luz de los crecientes retos a los que debe hacer frente 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. Dichos objetivos incluyen la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación, el intercambio de información y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la Unión. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades de la Unión que podrían complementar la acción de los Estados miembros, en particular en el caso de ciberincidentes y crisis transfronterizas a gran escala, al tiempo que se ha de tener en cuenta la importancia de mantener y seguir mejorando las capacidades nacionales de respuesta a las ciberamenazas de cualquier envergadura.

(7) Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos, las organizaciones y las empresas sobre las cuestiones de ciberseguridad. Además, dado que los ciberincidentes merman la confianza en los proveedores de servicios digitales y en el propio mercado único digital, en especial entre los consumidores, debe reforzarse la confianza ofreciendo información transparente sobre el nivel de seguridad de los productos, servicios y procesos de TIC y subrayando que incluso un elevado nivel de certificación de la ciberseguridad no puede garantizar que un producto o servicio o proceso de TIC sea completamente seguro. Esto puede verse facilitado por una certificación a escala de la Unión que establezca requisitos y criterios de evaluación de la ciberseguridad comunes para todos los mercados y sectores nacionales.

(8) La ciberseguridad no es una cuestión meramente tecnológica sino que en ella desempeña un papel igualmente importante el comportamiento humano. Por ello, debe promoverse enérgicamente la «ciberhigiene», a saber, medidas sencillas de rutina que, aplicadas con regularidad por los ciudadanos, las organizaciones y las empresas, minimizan su exposición a los riesgos derivados de las ciberamenazas.

(9) Con el fin de reforzar las estructuras de ciberseguridad de la Unión, es importante mantener y desarrollar las capacidades de los Estados miembros para responder globalmente a las ciberamenazas, incluidos los incidentes transfronterizos.

(10) Las empresas y los consumidores particulares deben disponer de información precisa sobre el nivel de garantía con el que se ha certificado la seguridad de sus productos, servicios y procesos de TIC. Al mismo tiempo, ningún producto o servicio de TIC es totalmente ciberseguro y se deben promover y priorizar normas básicas de ciberhigiene. Habida cuenta de la creciente disponibilidad de dispositivos de la internet de las cosas, hay una serie de medidas voluntarias que el sector privado puede adoptar para reforzar la confianza en la seguridad de los productos, servicios y procesos de TIC.

(11) A menudo, los modernos productos y sistemas de TIC integran una o varias tecnologías y componentes de terceros y se basan en ellos, por ejemplo, módulos de programas, bibliotecas o interfaces de programación de aplicaciones. Esta relación, llamada de «dependencia», puede presentar riesgos adicionales en materia de ciberseguridad, pues las vulnerabilidades de los componentes de terceros pueden afectar también a los productos, servicios y procesos de TIC. En gran número de casos, determinar y documentar dichas dependencias permite a los usuarios finales de los productos, servicios y procesos de TCI optimizar sus actividades de gestión relacionadas con la ciberseguridad mejorando, por ejemplo, los procedimientos que ponen a punto para detectar las vulnerabilidades en materia de ciberseguridad y ponerles remedio.

([5]) 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).

(12) Las organizaciones, fabricantes y proveedores implicados en el diseño y desarrollo de productos, servicios y procesos de TIC deben ser animadas a aplicar medidas desde las primeras fases del diseño y desarrollo que permitan proteger desde el principio y en la máxima medida posible la seguridad de tales productos, procesos y servicios, presuponer que se van a producir ataques y prever y limitar sus repercusiones («seguridad desde el diseño»). La seguridad se debe tener en cuenta durante todo el ciclo de vida del producto, servicio o proceso de TIC y los procesos de diseño y desarrollo deben evolucionar constantemente para reducir el riesgo de daños derivados de la explotación malintencionada.

(13) Las empresas, las organizaciones y el sector público que participan en el diseño deben configurar los productos, servicios o procesos de TIC de manera que se garantice un nivel de seguridad más elevado, lo que debe permitir que el primer usuario reciba una configuración por defecto que sea lo más segura posible (en lo sucesivo, «seguridad por defecto»), de modo que se reduzca la carga del usuario de configurar el producto, servicio o proceso de TIC de manera adecuada. La seguridad por defecto debe funcionar sin que sea necesaria una configuración minuciosa, unos conocimientos técnicos específicos o un comportamiento no evidente por parte del usuario y debe funcionar fácilmente y de manera fiable cuando se aplique. Si del análisis de riesgos y de manejabilidad, que se llevará a cabo caso por caso, se desprende que tal configuración no es viable, se deberá incitar a los usuarios a optar por la configuración más segura.

(14) El Reglamento (CE) n.º 460/2004 del Parlamento Europeo y del Consejo ([6]) creó ENISA con el objetivo de contribuir al establecimiento de un elevado y efectivo nivel de seguridad de las redes y de la información en la Unión y al desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las administraciones públicas. El Reglamento (CE) n.º 1007/2008 del Parlamento Europeo y del Consejo ([7]), prorrogó el mandato de ENISA hasta marzo de 2012. El Reglamento (UE) n.º 580/2011 del Parlamento Europeo y del Consejo ([8]) prorrogó nuevamente el mandato de ENISA hasta el 13 de septiembre de 2013. El Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo ha prorrogado el mandato de ENISA hasta el 19 de junio de 2020.

(15) 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 Unión Europea 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 ciudadanos en línea, el primer acto jurídico en el ámbito de la ciberseguridad de la Unión fue adoptado en 2016, fue la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([9]). La Directiva (UE) 2016/1148 instauró una serie de 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 de la economía y la sociedad, como la energía, los transportes, el agua potable, el suministro y la distribución, la banca, las infraestructuras de los mercados financieros, la sanidad o las infraestructuras digitales, así como para los proveedores de servicios digitales clave (motores de búsqueda, servicios en la nube y mercados en línea).

Se atribuyó un papel clave a ENISA para respaldar la aplicación de dicha Directiva. Además, la lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, que contribuye al objetivo general de conseguir un elevado nivel de ciberseguridad. También contribuyen al elevado nivel de ciberseguridad en el mercado único digital otros actos jurídicos, como el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([10]) y las Directivas 2002/58/CE ([11]) y (UE) 2018/1972 ([12]) del Parlamento Europeo y del Consejo.

([6]) 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).

([7]) 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).

([8]) 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).

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

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

([11]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([12]) Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

(16) Desde la adopción de la Estrategia de Ciberseguridad de la Unión Europea en 2013 y la última revisión del mandato de ENISA, el contexto político general ha cambiado considerablemente y el contexto mundial ha pasado a ser más incierto y menos seguro. En este contexto y en el marco de la positiva evolución del cometido de ENISA a lo largo de los años como punto de referencia en materia de asesoramiento y conocimientos y como facilitadora de la coordinación y el desarrollo de capacidades, así como 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 nuevo ecosistema de la ciberseguridad y garantizar que contribuya eficazmente a configurar la respuesta de la Unión a los desafíos de ciberseguridad derivados de la transformación radical de las amenazas, para lo cual, como reconoció la evaluación de ENISA, el mandato actual resulta insuficiente.

(17) ENISA tal como se establece en el presente Reglamento debe suceder a ENISA tal como fue creada por el Reglamento (UE) n.º 526/2013. ENISA debe llevar a cabo las tareas que le confiere el presente Reglamento y otros 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 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 tanto entre los Estados miembros, como entre los Estados miembros y las instituciones, órganos y organismos de la Unión.

(18) En el marco de la Decisión 2004/97/CE, Euratom, tomada de común acuerdo por los representantes de los Estados miembros, reunidos a nivel de jefes de Estado o de Gobierno ([13]), 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 ENISA debe ofrecer las mejores condiciones posibles para su funcionamiento correcto y eficaz. Para el desempeño correcto y eficaz de sus funciones, para atraer y conservar al personal y para establecer contactos con el exterior de manera más eficaz, es imperativo que ENISA 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 ENISA y el Estado miembro anfitrión, cuya celebración ha de contar con la aprobación del Consejo de Administración de ENISA.

(19) En vista de los crecientes riesgos y amenazas en materia de ciberseguridad a los que debe hacer frente la Unión, deben incrementarse los recursos financieros y humanos asignados a ENISA, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crucial en el ecosistema de organizaciones que defienden el ecosistema digital de la Unión, a fin de permitir que ENISA pueda desempeñar eficazmente las tareas que le encomienda el presente Reglamento.

(20) ENISA 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, la transparencia de sus métodos de funcionamiento y su diligencia en el desempeño de sus tareas. ENISA debe apoyar activamente los esfuerzos nacionales y contribuir proactivamente a los esfuerzos de la Unión y desempeñar sus funciones cooperando plenamente con las instituciones, órganos y organismos de la Unión y con los Estados miembros, evitando la duplicación de tareas y promoviendo las sinergias. Además, ENISA debe apoyarse en las aportaciones del sector privado y otras partes interesadas pertinentes y en la cooperación con tales agentes.

La manera en que ENISA debe alcanzar sus objetivos se debe definir a través de un conjunto de tareas que permita cierta flexibilidad en su funcionamiento.

(21) Para poder prestar un apoyo adecuado a la cooperación operativa entre los Estados miembros, ENISA debe seguir reforzando sus capacidades y destrezas técnicas y humanas. ENISA debe reforzar sus conocimientos técnicos y capacidades. ENISA y los Estados miembros pueden, de forma voluntaria, elaborar programas para la comisión de servicios de expertos nacionales en ENISA, la creación de contingentes de expertos y el intercambio de personal.

(22) ENISA debe prestar asistencia a la Comisión mediante asesoramiento, dictámenes y análisis en todos los asuntos de la Unión relacionados con la formulación, la actualización y la revisión de políticas y disposiciones legislativas en el ámbito de la ciberseguridad y sus aspectos sectoriales para potenciar la pertinencia de las políticas y la legislación de la Unión que presenten aspectos relacionados con la ciberseguridad y permitir la coherencia en su aplicación a nivel nacional. La Agencia debe actuar como punto de referencia de asesoramiento y conocimientos en relación con las iniciativas políticas y legislativas sectoriales de la Unión, cuando intervengan cuestiones relacionadas con la ciberseguridad. ENISA debe informar periódicamente al Parlamento Europeo de sus actividades.

([13]) Decisión 2004/97/CE, Euratom adoptada de común acuerdo por los Representantes de los Estados miembros, reunidos a escala de Jefes de Estado o de Gobierno, de 13 de diciembre de 2003, relativa a la fijación de las sedes de determinadas oficinas y agencias de la Unión Europea (DO L 29 de 3.2.2004, p. 15).

(23) El núcleo público de la internet abierta, consistente en sus protocolos e infraestructura principales, que constituyen un bien público mundial, posibilita la funcionalidad esencial de internet en su conjunto, y en él se sustenta su funcionamiento normal. ENISA debe promover la seguridad una internet pública esencial y abierta y la estabilidad de su funcionamiento, lo que incluye, a título meramente enunciativo, sus protocolos esenciales (en particular, DNS, BGP e IPv6), el funcionamiento del sistema de nombres de dominio (incluido el funcionamiento de todos los dominios de nivel superior) y el funcionamiento de la zona raíz.

(24) La principal tarea de ENISA es promover la aplicación coherente del marco jurídico pertinente, en particular la aplicación efectiva de la Directiva (UE) 2016/1148 y otros instrumentos jurídicos pertinentes que contienen disposiciones en materia de ciberseguridad, lo 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.

(25) ENISA debe asistir a los Estados miembros y a las instituciones, órganos y organismos de la Unión en sus esfuerzos por crear 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, ENISA debe prestar apoyo al establecimiento y mejora de los equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «CSIRT», por sus siglas en inglés de «computer security incident response teams») nacionales y de la Unión previstos en la Directiva (UE) 2016/1148 con vistas a alcanzar un elevado nivel común de madurez en la Unión. Las actividades realizadas por ENISA en relación con las capacidades operativas de los Estados miembros deben respaldar activamente las acciones emprendidas por los Estados miembros para el cumplimiento de sus obligaciones en virtud de la Directiva (UE) 2016/1148 y no deben, por tanto, sustituirlas.

(26) ENISA también debe prestar asistencia en la elaboración y actualización de las estrategias en materia de seguridad de las redes y los sistemas de información a escala de la Unión y, previa solicitud, a escala de los Estados miembros, en particular, en materia de ciberseguridad, y debe promover la difusión de dichas estrategias y hacer un seguimiento de los avances en su aplicación. Asimismo, ENISA debe ofrecer aportaciones para satisfacer la necesidad de cursos y material de formación, en particular a los organismos públicos y, cuando proceda, y en gran medida, «formar formadores», sobre la base del Marco de Competencias Digitales para los Ciudadanos con el fin de ayudar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a desarrollar sus propias capacidades de formación.

(27) ENISA debe apoyar a los Estados miembros en el ámbito de la sensibilización y la educación en materia de ciberseguridad facilitando una coordinación más estrecha y el intercambio de mejores prácticas entre los Estados miembros. Dicho apoyo debe consistir en la creación de una red de puntos de contacto nacionales en materia de educación y en el establecimiento de una plataforma de formación sobre ciberseguridad. La red de puntos de contacto nacionales en materia de educación puede funcionar en el marco de la red de funcionarios de enlace nacionales y servir de punto de partida para la coordinación futura dentro de los Estados miembros.

(28) ENISA debe asistir al Grupo de cooperación creado por la Directiva (UE) 2016/1148 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, así como en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes.

(29) Con el fin de estimular la cooperación entre los sectores público y privado y dentro del sector privado, en particular para apoyar la protección de las infraestructuras críticas, ENISA debe animar a que los sectores intercambien información entre sí y también en su propio seno, en particular aquellos 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).

(30) Mientras el posible impacto negativo de las vulnerabilidades detectadas en los productos, servicios y procesos de TIC siga aumentando, será de vital importancia identificarlas y subsanarlas con el fin de reducir los riesgos generales en materia de ciberseguridad. Se ha demostrado que la cooperación entre organizaciones, fabricantes o proveedores de productos, servicios y procesos de TIC vulnerables y los miembros de la comunidad investigadora en materia de ciberseguridad y las autoridades encargadas de la identificación de dichas vulnerabilidades aumenta considerablemente la tasa de identificación y corrección de las vulnerabilidades detectadas en los productos, servicios y procesos de TIC. La divulgación coordinada de vulnerabilidades es un proceso estructurado de cooperación en el que se informa al propietario del sistema de información de las vulnerabilidades detectadas, lo que ofrece a la organización la oportunidad de identificar y subsanar una vulnerabilidad antes de que la información detallada relacionada con esta se haga pública o pueda divulgarse a terceros. Este proceso facilita además la coordinación entre el identificador y la organización en lo que respecta a la publicación de dichas vulnerabilidades. Las políticas de la divulgación coordinada de vulnerabilidades pueden desempeñar un papel importante en los esfuerzos de los Estados miembros por mejorar la ciberseguridad.

(31) ENISA debe agregar y analizar, compartidos de forma voluntaria, los informes nacionales de los CSIRT y del equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) establecido por el Acuerdo entre el Parlamento Europeo, el Consejo Europeo, el Consejo de la Unión Europea, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo, el Tribunal de Cuentas Europeo, el Servicio Europeo de Acción Exterior, el Comité Económico y Social Europeo, el Comité Europeo de las Regiones y el Banco Europeo de Inversiones sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) ([14]), a los efectos de contribuir al establecimiento de unos procedimientos, un lenguaje y una terminología comunes para el intercambio de información. En este contexto, ENISA debe fomentar la participación del sector privado, en el marco de la Directiva (UE) 2016/1148, que establece las bases para el intercambio voluntario de información técnica a nivel operativo dentro de la red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red CSIRT») creada por dicha Directiva.

(32) ENISA debe contribuir a aportar una respuesta a nivel de la Unión en caso de incidentes y crisis transfronterizos a gran escala relacionados con la ciberseguridad. Esta tarea debe desempeñarse conforme al mandato de ENISA en virtud del presente Reglamento y a una fórmula que acordarán los Estados miembros en el contexto de la Recomendación (UE) 2017/1584 ([15]) de la Comisión y a las conclusiones del Consejo de 26 de junio de 2018 sobre la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala. La citada tarea 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 entre los responsables políticos de gestionar la crisis. Por otra parte, ENISA debe apoyar la cooperación operativa entre Estados miembros, a petición de uno o más Estados miembros, para el tratamiento de incidentes desde una perspectiva técnica facilitando el intercambio de soluciones técnicas pertinentes entre los Estados miembros y aportando información a las comunicaciones públicas. ENISA debe apoyar la cooperación operativa ensayando las disposiciones de esa cooperación a través de ejercicios periódicos de ciberseguridad.

(33) Al apoyar la cooperación operativa, ENISA debe hacer uso de las competencias técnicas y operativas disponibles del CERT-UE a través de una cooperación estructurada. La cooperación estructurada puede permitir acumular conocimientos a ENISA. Cuando proceda, deben establecerse disposiciones específicas adecuadas entre las dos entidades para definir los aspectos prácticos de dicha cooperación y evitar la duplicación de actividades.

(34) Al desempeñar sus tareas de apoyo de la cooperación operativa dentro de la red de CSIRT, ENISA debe poder prestar ayuda a los Estados miembros si estos se la piden, por ejemplo, asesorándolos sobre el modo de mejorar sus capacidades para prevenir, detectar y responder ante incidentes, facilitando la gestión técnica de incidentes que tengan un impacto significativo o sustancial o garantizando que se realicen análisis de ciberamenazas e incidentes. ENISA debe facilitar la gestión técnica de los incidentes que tengan un impacto significativo o sustancial, en particular, apoyando el intercambio voluntario 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 (UE) 2017/1584 recomienda que los Estados miembros cooperen de buena fe y compartan entre ellos y con ENISA información sobre las crisis e incidentes a gran escala relacionados con la ciberseguridad sin demora indebida. Dicha información debe servir de ayuda a ENISA en el desempeño de sus funciones de apoyo a la cooperación operativa.

(35) Dentro de la cooperación regular a nivel técnico para ayudar a la Unión a conocer la situación, ENISA, en estrecha cooperación con los Estados miembros, debe elaborar periódicamente un informe detallado de situación técnica en materia de ciberseguridad de la UE sobre incidentes y ciberamenazas, 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 nacionales sobre la seguridad de las redes y sistemas de información (en lo sucesivo, «puntos de contacto únicos») previstos en la Directiva (UE) 2016/1148 (ambos de forma voluntaria), el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y, cuando proceda, el Centro de Análisis de Inteligencia de la Unión Europea (UE-INTCEN) del Servicio Europeo de Acción Exterior (. Dicho informe debe ponerse a disposición del Consejo, la Comisión, la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y la red de CSIRT.

(36) El apoyo de ENISA a las investigaciones técnicas *ex post* en relación con incidentes con efectos significativos facilitado a petición de los Estados miembros afectados debe centrarse en la prevención de incidentes futuros. Los Estados miembros afectados deben proporcionar la información y asistencia necesarias para que ENISA pueda apoyar de forma efectiva la investigación técnica *ex post*.

([14]) DO C 12 de 13.1.2018, p. 1.

([15]) Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

(37) Los Estados miembros podrán invitar a las empresas afectadas por el incidente a colaborar facilitando a ENISA toda la información y asistencia necesarias, sin perjuicio de su derecho a proteger la información sensible desde el punto de vista comercial y que afecte a la seguridad pública.

(38) 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 a las instituciones, órganos y organismos de la Unión, ENISA necesita analizar los riesgos actuales y emergentes de ciberseguridad. A tal efecto, ENISA, 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, ENISA debe apoyar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a la hora de detectar nuevos riesgos relacionados con la ciberseguridad y prevenir los incidentes, mediante la realización de análisis de ciberamenazas, vulnerabilidades e incidentes.

(39) Con el fin de aumentar la resiliencia de la Unión, ENISA debe impulsar conocimientos en el ámbito de la ciberseguridad de las infraestructuras prestando apoyo, en particular, a los sectores recogidos en el anexo II de la Directiva (UE) 2016/1148 y los que utilicen los proveedores de servicios digitales que figuran en el anexo III de dicha Directiva, ofreciendo asesoramiento y orientaciones e intercambiando mejores prácticas. Con el fin de facilitar el acceso a una información mejor estructurada sobre los riesgos relacionados con la ciberseguridad y las posibles soluciones, ENISA 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 Unión. Facilitar el acceso a una información mejor estructurada sobre los riesgos relacionados con la ciberseguridad y las posibles soluciones también puede ayudar a los Estados miembros a consolidar sus capacidades, a alinear sus prácticas y, por ende, a mejorar su resiliencia general frente a los ciberataques.

(40) ENISA debe contribuir a la sensibilización del público sobre los riesgos relacionados con la ciberseguridad, en particular mediante una campaña de sensibilización a nivel europeo y la promoción de la educación, y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos, organizaciones y empresas. ENISA debe contribuir asimismo a promover las mejores prácticas y soluciones, incluidas la ciberhigiene y la ciberalfabetización de los ciudadanos, a nivel de ciudadanos, organizaciones y empresas mediante la recogida y el análisis de la información disponible públicamente relativa a incidentes significativos, y mediante la elaboración y publicación de informes y orientaciones para ciudadanos, organizaciones y empresas y mejorar el nivel general de preparación y resiliencia. ENISA también debe trabajar para proporcionar a los consumidores la correspondiente información acerca de los esquemas de certificación aplicables, por ejemplo, ofreciendo orientaciones y recomendaciones. ENISA debe además organizar, en consonancia con el Plan de Acción de Educación Digital establecido en la Comunicación de la Comisión de 17 de enero de 2018 y en colaboración con los Estados miembros y las instituciones, agencias y organismos de la Unión, campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y la alfabetización digital y a concienciar sobre las ciberamenazas potenciales, incluyendo actividades criminales en línea como los ataques por suplantación de identidad (phishing), las redes infectadas (botnets) o los fraudes bancarios y financieros, e incidentes de fraude en materia de datos, así como dar consejos básicos en materia de autenticaciones multifactores, correcciones, cifrado, anonimización y protección de datos.

(41) ENISA debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos y el uso seguro de los servicios, promoviendo a nivel de la Unión la seguridad y la protección de la intimidad desde la concepción de los mismos. Para lograr ese objetivo, ENISA debe aprovechar al máximo las mejores prácticas y experiencias existentes, en especial las de las instituciones académicas y de los investigadores en materia de seguridad informática.

(42) 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, ENISA 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.

(43) ENISA debe contribuir a los esfuerzos de la Unión de cooperar con organismos internacionales y en marcos de cooperación internacional pertinentes en el ámbito de la ciberseguridad. En particular, ENISA debe contribuir, cuando proceda, a la cooperación con organismos tales como la OCDE, la OSCE y la OTAN. Dicha cooperación podría incluir la realización de ejercicios conjuntos de ciberseguridad y la coordinación conjunta de la respuesta a incidentes. Dichas actividades deben realizarse respetando plenamente los principios de inclusión, reciprocidad y autonomía del proceso decisorio de la Unión, sin perjuicio del carácter específico de la política de seguridad y defensa de los Estados miembros.

(44) Para asegurar que cumple plenamente sus objetivos, ENISA debe permanecer en contacto con las correspondientes autoridades de supervisión de la Unión y otras autoridades competentes de la Unión, instituciones, órganos y organismos de la Unión, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, Agencia Europea de Defensa (AED), la Agencia del Sistema Global de Navegación por Satélite Europeo (Agencia del GNSS Europeo), el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), la Agencia Europea para la Gestión Operativa de los Sistemas Informáticos de Gran Magnitud en el espacio de libertas, seguridad y justicia (eu-LISA), el Banco Central Europeo (BCE), la Autoridad Bancaria Europea (ABE), el Comité Europeo de Protección de Datos, la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (ACER), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la Unión relacionado con la ciberseguridad.

ENISA 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 Consultivo de ENISA. En sus relaciones con las autoridades encargadas de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en su trabajo, ENISA debe respetar los canales de información y las redes existentes.

(45) Pueden establecerse asociaciones con instituciones académicas que desarrollen iniciativas de investigación en los ámbitos pertinentes, y deben contar con cauces apropiados de las aportaciones de las organizaciones de consumidores y otras organizaciones, que deben tenerse en cuenta.

(46) ENISA, 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 (UE) 2016/1148. Además, ENISA 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 CSIRT, teniendo siempre debidamente en cuenta los procedimientos operativos estándar de la red de CSIRT.

(47) Con el fin de aumentar la preparación de la Unión para una respuesta a los incidentes, ENISA 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 Unión en la organización de ejercicios. Los ejercicios exhaustivos de seguridad a gran escala en el que se incluyan elementos técnicos, operativos y estratégicos deben organizarse cada dos años. Además, ENISA debe poder organizar periódicamente ejercicios menos exhaustivos con el mismo objetivo de mejorar la preparación de la Unión para responder a los incidentes.

(48) ENISA 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. ENISA debe aprovechar las buenas prácticas existentes y 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 (marco europeo de certificación de la ciberseguridad), con el fin de aumentar la transparencia de la garantía de la ciberseguridad de los productos, servicios y procesos de TIC y reforzar así la confianza en el mercado interior digital, así como su competitividad.

(49) Unas políticas de ciberseguridad eficientes deben basarse en métodos de evaluación de riesgos bien elaborados, 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, ENISA debe apoyar la cooperación entre las partes interesadas a escala de la Unión y facilitar 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.

(50) ENISA debe alentar a los Estados miembros, a los fabricantes o los proveedores de productos, servicios o procesos de TIC 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 y deben dar incentivos para ello. En particular, los fabricantes y proveedores de productos, servicios o procesos de TIC deben aportar las actualizaciones necesarias y recuperar, retirar o reciclar los productos, servicios o procesos de TIC que no cumplan las normas de ciberseguridad, mientras que los importadores y distribuidores deben asegurarse de que los productos, servicios y procesos de TIC que introduzcan en el mercado de la Unión cumplen los requisitos aplicables y no supongan un riesgo para los consumidores de la Unión.

(51) En cooperación con las autoridades competentes, ENISA debe poder difundir información relativa al nivel de ciberseguridad de los productos, servicios y procesos de TIC ofrecidos en el mercado interior, y emitir advertencias dirigidas a los fabricantes y los proveedores de productos, servicios o procesos de TIC solicitándoles que mejoren la seguridad de los mismos, incluida la ciberseguridad.

(52) ENISA 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, ENISA debe consultar asimismo a los grupos de usuarios pertinentes. Más concretamente, puede establecerse una cooperación con el Consejo Europeo de Investigación y el Instituto Europeo de Innovación y Tecnología, así como con el Instituto de Estudios de Seguridad de la Unión Europea.

(53) ENISA debe consultar de forma regular a organizaciones de normalización, en particular a organizaciones de normalización europeas, a la hora de preparar los esquemas europeos de certificación de la ciberseguridad.

(54) Las ciberamenazas tienen un alcance mundial. Es necesaria una cooperación internacional más estrecha para mejorar las normas de ciberseguridad, incluida la necesidad de definir normas de comportamiento comunes, la adopción de códigos de conducta, el uso de normas internacionales 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, y promueva un enfoque mundial común al respecto. A tal efecto, ENISA 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 correspondientes instituciones, órganos y organismos de la Unión.

(55) ENISA 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 Unión en materias que correspondan al mandato de ENISA.

(56) Es razonable y recomendable aplicar determinados principios relativos a la gobernanza de ENISA para cumplir con la declaración conjunta y el enfoque común aprobados en julio de 2012 por el Grupo de trabajo interinstitucional sobre las agencias descentralizadas, cuya finalidad es la racionalización las actividades de las agencias descentralizadas y la mejora de su funcionamiento. Las recomendaciones de la declaración conjunta y el enfoque común también han de quedar reflejados, cuando proceda, en los programas de trabajo de ENISA, sus evaluaciones y sus prácticas administrativas y de presentación de informes.

(57) El Consejo de Administración, integrado por los representantes de Estados miembros y de la Comisión, debe establecer la orientación general del funcionamiento de ENISA 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 ENISA, adoptar el documento único de programación de ENISA, adoptar su propio reglamento interno, nombrar al director ejecutivo y decidir la prórroga y terminación del mandato del director ejecutivo.

(58) Para que ENISA 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 y de experiencia adecuadas. 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.

(59) Para un buen funcionamiento de ENISA, 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 anual de ENISA, 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 ENISA que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de ENISA y ejecutar el presupuesto. Además, el director ejecutivo debe tener la posibilidad de crear grupos de trabajo *ad hoc* para que examinen asuntos concretos, en particular los de índole científica, técnica, jurídica o socioeconómica. En particular, en relación con la preparación de una propuesta de esquema específica de certificación europea de ciberseguridad (en lo sucesivo, «propuesta de esquema»), la creación de un grupo de trabajo *ad hoc* se considera necesaria. 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 y de género, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones, órganos y organismos de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información.

(60) 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, el Comité Ejecutivo debe examinar en detalle la información pertinente, explorar las opciones disponibles y ofrecer asesoramiento y soluciones para preparar las decisiones del Consejo de Administración.

(61) ENISA debe contar con un Grupo Consultivo de ENISA 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 Consultivo de ENISA, 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 ENISA. El Grupo Consultivo de ENISA debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo anual. La composición del Grupo Consultivo de ENISA y las tareas asignadas a este grupo deben garantizar una representación suficiente de las partes interesadas en los trabajos de ENISA.

(62) Debe crearse el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad para ayudar a ENISA y a la Comisión a facilitar la consulta de las partes interesadas pertinentes. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad debe estar compuesto por miembros que representen a la industria en una proporción equilibrada, tanto del lado de la demanda como de la oferta de productos y servicios de TIC, y entre ellos, en particular, las pymes, los proveedores de servicios digitales, los organismos de normalización europeos e internacionales, los organismos nacionales de acreditación, las autoridades de supervisión de la protección de datos y los organismos de evaluación de la conformidad en virtud del Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([16]), el mundo académico y las organizaciones de consumidores.

(63) ENISA debe instaurar normas para la prevención y gestión de los conflictos de intereses. ENISA 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 ([17]). Los datos personales deben ser tratados por ENISA de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([18]),. ENISA debe cumplir las disposiciones aplicables a las instituciones, órganos y organismos 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 Unión Europea (ICUE).

(64) Con el fin de garantizar la plena autonomía e independencia de ENISA 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 ENISA. Es primordial que ENISA disponga de un presupuesto adecuado de modo que disponga de la capacidad suficiente para cumplir todos sus cometidos y objetivos, que cada vez son mayores. La mayor parte del personal de ENISA debe estar dedicado directamente a la ejecución operativa del mandato de ENISA. Debe permitirse que el Estado miembro anfitrión, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de ENISA. 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 ENISA para garantizar la transparencia y la responsabilidad.

(65) La certificación de la ciberseguridad desempeña un importante papel a la hora de aumentar la confianza y la seguridad en los productos, servicios y procesos 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, servicios y procesos ofrecen un determinado nivel 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 (UE) 2016/1148 resulta crítica la certificación de la ciberseguridad.

([16]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

([17]) 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).

([18]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

(66) 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, servicios y procesos 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 Unión es otra de las carencias que padece el mercado único de la ciberseguridad. Esto hace difícil que las empresas europeas compitan a nivel nacional, de la Unión y mundial. Ello también 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 comunicación de 2017 sobre la aplicación de la Estrategia para el Mercado Único Digital-Un Mercado Único Digital conectado para todos, 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 interior.

(67) En la actualidad, la certificación de la ciberseguridad de los productos, servicios y procesos de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de esquemas impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de certificación de la ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos, servicios y procesos TIC en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales, con el correspondiente aumento de sus costes. Por otra parte, aun cuando están surgiendo nuevos esquemas, 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 esquemas existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real, lo que crea dificultades a los mecanismos de reconocimiento mutuo dentro de la Unión.

(68) Se han realizado esfuerzos en el pasado para velar por el reconocimiento mutuo de los certificados dentro de la Unión, 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 algunos Estados miembros. Esto ha limitado la eficacia del ARM del SOG-IS desde el punto de vista del mercado interior.

(69) Por consiguiente, es necesario adoptar un planteamiento común y establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar esquemas europeos de certificación de la ciberseguridad y permita que los certificados de ciberseguridad europeos y las declaraciones de conformidad de la UE de productos, servicios o procesos de TIC sean reconocidos y usados en todos los Estados miembros. A este respecto, es esencial basarse en los esquemas nacionales e internacionales existentes, así como en los sistemas de reconocimiento mutuo, en particular el SOG-IS, y permitir una transición fluida de los esquemas existentes bajo dichos sistemas a los esquemas del nuevo marco europeo de certificación de la ciberseguridad. El marco europeo de certificación de la ciberseguridad. debe tener un doble objetivo. Primero, debe contribuir a aumentar la confianza en los productos, servicios y procesos de TIC que hayan sido certificados con arreglo a los esquemas europeos de certificación de la ciberseguridad. Segundo, evitar la multiplicación de los esquemas 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 esquemas europeos de certificación de la ciberseguridad 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 Unión al respecto.

(70) El marco europeo de certificación de la ciberseguridad debe implantarse de forma uniforme en todos los Estados miembros, a fin de evitar la práctica de escoger entre ellos en función de las diferencias en los niveles de exigencia en diferentes Estados miembros.

(71) Los esquemas europeos de certificación de la ciberseguridad deben basarse en los ya existentes a nivel nacional e internacional y, de ser necesario, en especificaciones técnicas de foros y consorcios, aprendiendo de los puntos fuertes actuales y evaluando y corrigiendo los puntos débiles.

(72) Se necesitan soluciones de ciberseguridad flexibles para que la industria vaya por delante de las ciberamenazas y, por tanto, cualquier esquema de certificación debe concebirse de tal manera que se evite el riesgo de quedarse rápidamente desfasado.

(73) La Comisión debe estar facultada para adoptar esquemas europeos de certificación de la ciberseguridad relativos a grupos específicos de productos, servicios y procesos de TIC. Estos esquemas 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 esquemas de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del presente Reglamento. No obstante, los organismos responsables de dichos esquemas deben poder proponer a la Comisión que los tome en consideración como base para su aprobación como esquemas europeos de certificación de la ciberseguridad.

(74) Las disposiciones del presente Reglamento deben entenderse sin perjuicio de la legislación de la Unión que fija normas específicas sobre la certificación de productos, servicios y procesos de TIC. En particular, el Reglamento (UE) 2016/679 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, servicios y procesos de TIC. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del Reglamento (UE) 2016/679, incluso cuando dichas operaciones se encuentran integradas en productos, servicios y procesos de TIC.

(75) El objetivo de los esquemas europeos de certificación de la ciberseguridad debe ser garantizar que los productos, servicios y procesos de TIC certificados con arreglo a un esquema 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, servicios y procesos a lo largo de su ciclo de vida, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle los requisitos de ciberseguridad relativos a todos los productos, servicios y procesos de TIC en el presente Reglamento. Los productos, servicios y procesos de TIC y las necesidades de ciberseguridad relativas a dichos productos, servicios y procesos son tan dispares que es muy difícil elaborar unos requisitos de ciberseguridad generales que sean válidos en todas las circunstancias. Por lo tanto, es necesario adoptar un concepto amplio y general de la ciberseguridad a efectos de la certificación, que debe ser complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los esquemas europeos de certificación de ciberseguridad. Las disposiciones con que se lograrán tales objetivos para determinados productos, servicios y procesos de TIC deben especificarse luego con más detalle a nivel de cada esquema de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas cuando no se disponga de normas apropiadas.

(76) Las especificaciones técnicas que deben utilizarse en un esquema europeo de certificación de la ciberseguridad deben respetar los requisitos establecidos en el anexo II del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([19]). No obstante, podrían considerarse necesarias algunas variaciones con respecto a estos requisitos en casos debidamente justificados en los que dichas especificaciones técnicas vayan a utilizarse en un esquema europeo de certificación de la ciberseguridad de nivel de garantía «elevado». Los motivos que justifican tales variaciones deben hacerse públicos.

(77) La evaluación certificada de la conformidad es el procedimiento 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 procedimiento es necesario un tercero independiente, que no sea el fabricante del producto ni el proveedor del producto, servicio o proceso de TIC que está siendo evaluado. Un certificado europeo de ciberseguridad debe ser expedido tras un procedimiento de evaluación exitoso de un producto, servicio o proceso de TIC. Un certificado europeo de ciberseguridad debe considerarse una confirmación de que la evaluación se ha llevado a cabo de forma apropiada. En función del nivel de garantía, el esquema europeo de certificación de la 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, servicios y procesos de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos, servicios y procesos de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

(78) La elección del nivel adecuado de certificación y de los requisitos de seguridad asociados por parte de los usuarios de certificados europeos de ciberseguridad debe basarse en el análisis del riesgo asociado con el uso de productos, servicios o procesos de TIC. Por tanto, el nivel de garantía debe así reflejar el nivel de riesgo asociado con el uso previsto de un producto, servicio o proceso de TIC.

([19]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

(79) Un esquema 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, servicios y procesos de TIC (autoevaluación de la conformidad). En tales casos, basta con que el fabricante o proveedor de productos, servicios y procesos de TIC lleve a cabo por sí mismo todas las comprobaciones que garanticen la conformidad de los productos, servicios o procesos de TIC con el esquema de certificación europea de ciberseguridad. Este tipo de evaluación de la conformidad debe considerarse adecuado para productos, servicios o procesos de TIC poco complejos que presentan un nivel de riesgo bajo para el público, por ejemplo, cuando el diseño y el mecanismo de producción son sencillos. Asimismo, la autoevaluación de la conformidad debe estar permitida para los productos, servicios o procesos de TIC, únicamente cuando corresponden al nivel de garantía «básico».

(80) Un esquema europeo de certificación de la ciberseguridad puede permitir la autoevaluación de la conformidad y las certificaciones de los productos, servicios o procesos de TIC. En este caso, el esquema debe establecer medios claros y comprensibles para que los consumidores u otros usuarios puedan diferenciar los productos, servicios o procesos de TIC respecto de los cuales el fabricante o proveedor de productos, servicios o procesos de TIC es responsable de la evaluación, y los productos, servicios o procesos de TIC certificados por un tercero.

(81) El fabricante o proveedor de productos, servicios o procesos 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 un documento que determina si un producto, servicio o proceso de TIC específico cumple los requisitos del esquema europeo de certificación de la ciberseguridad. Al expedir y firmar la declaración de conformidad de la UE, el fabricante o proveedor de productos, servicios o procesos de TIC asume la responsabilidad de que el producto, servicio o proceso de TIC cumple los requisitos legales del esquema europeo de certificación de la ciberseguridad. Debe presentarse una copia de la declaración de conformidad de la UE a la autoridad nacional de certificación de la ciberseguridad y a ENISA.

(82) Los fabricantes o proveedores de productos, servicios o procesos de TIC deben poner a disposición de la autoridad nacional de certificación de la seguridad competente, por un plazo previsto en el esquema europeo específico de certificación de la ciberseguridad, la declaración de conformidad de la UE, la documentación técnica, y toda la información pertinente relativa a la conformidad de los productos, servicios o procesos de TIC con el esquema europeo de certificación de la ciberseguridad de que se trate. La documentación técnica debe especificar los requisitos aplicables en virtud del esquema y debe contemplar, en la medida en que sea pertinente para la autoevaluación de la conformidad, el diseño, la fabricación y el funcionamiento del producto, servicio o proceso 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 aplicables en virtud de dicho esquema.

(83) La gobernanza del marco europeo de certificación de la ciberseguridad tiene en cuenta la participación de los Estados miembros así como la participación adecuada de las partes interesadas y determina el papel de la Comisión en la planificación y la propuesta, la solicitud, la preparación, la adopción y la revisión de los esquemas europeos de certificación de la ciberseguridad.

(84) La Comisión debe elaborar, con el apoyo del Grupo Europeo de Certificación de la Ciberseguridad (GECC) y del Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad y tras una consulta abierta y amplia, un programa de trabajo evolutivo de la Unión para los esquemas europeos de certificación de la ciberseguridad y debe publicarlo en forma de instrumento no vinculante. El programa de trabajo evolutivo de la Unión debe constituir un documento estratégico que permita en particular a la industria, a las autoridades nacionales y a los organismos de normalización prepararse de antemano para los futuros esquemas europeos de certificación de la ciberseguridad.

El programa de trabajo evolutivo de la Unión debe incluir una perspectiva plurianual de las solicitudes de las propuestas de esquemas que la Comisión tenga intención de presentar a ENISA para su preparación, sobre la base de motivos específicos. La Comisión debe tener en cuenta este programa de trabajo evolutivo durante la elaboración de su plan evolutivo para la normalización de las TIC y de las peticiones de normalización dirigidas a los organismos europeos de normalización. Habida cuenta de la rapidez en la introducción y asimilación de las nuevas tecnologías, de la aparición de riesgos relacionados con la ciberseguridad anteriormente desconocidos o de la evolución de la legislación y de los mercados, la Comisión o el GECC debe estar facultado para solicitar a ENISA que prepare propuestas de esquemas que no se incluían en el programa de trabajo evolutivo de la Unión. En tales casos, la Comisión y el GECC también deben evaluar la necesidad de dicha solicitud teniendo presentes los fines y objetivos generales del presente Reglamento y garantizando la continuidad por lo que respecta a la planificación y el uso de recursos por ENISA.

Tras recibir una solicitud, ENISA debe preparar sin demora indebida propuestas de esquemas para productos, servicios o procesos de TIC específicos. La Comisión debe evaluar los efectos positivos y negativos de su solicitud en el mercado concreto de que se trate, en especial en las pymes, en la innovación, en los obstáculos a la entrada a dicho mercado y en los costes para los usuarios finales. A continuación, la Comisión, sobre la base de la propuesta de esquema presentada por ENISA, debe estar facultada para adoptar el esquema 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 esquemas 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 esquema concreto.

Entre ellos deben figurar el alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos, servicios y procesos de TIC que cubre, la especificación detallada de los requisitos de ciberseguridad, por ejemplo haciendo referencia a normas o especificaciones técnicas, los criterios y métodos de evaluación específicos, así como el nivel de garantía previsto («básico», «sustancial» o «elevado») y los niveles de evaluación cuando proceda. ENISA debe poder rechazar una solicitud del GECC. Corresponde al Consejo de Administración adoptar tales decisiones y deben estar debidamente motivadas.

(85) ENISA debe encargarse del mantenimiento de un sitio web que facilite información y publicidad sobre los esquemas europeos de certificación de la ciberseguridad, que debe incluir, entre otras cosas, las solicitudes para preparar una propuesta de esquema 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. El sitio web también debe proporcionar información sobre los certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE expedidos en virtud del presente Reglamento, incluyendo información relativa a la retirada y expiración de dichos certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE. El sitio web debe indicar asimismo aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

(86) El nivel de garantía de un esquema europeo de certificación constituye la base para confiar en que un producto, servicio o proceso de TIC cumple los requisitos sobre seguridad de un esquema europeo de certificación de la ciberseguridad específico. Con el fin de garantizar la coherencia del marco europeo de certificación de la ciberseguridad, un esquema 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 esquema. Cada certificado europeo de ciberseguridad 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 deberían prever el rigor y la amplitud correspondientes para la evaluación del producto, servicio o proceso de TIC y deberían determinarse por referencia a especificaciones técnicas, normas y procedimientos relacionados, incluidos los controles técnicos, cuyo objetivo es reducir o evitar incidentes. Cada nivel de garantía debe ser coherente en los distintos ámbitos sectoriales a los que se aplica la certificación.

(87) Un esquema europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y lo exhaustivo de la metodología de evaluación utilizada. Los niveles de evaluación deben equivaler a uno de los niveles de garantía y deben asociarse con una combinación adecuada de componentes de garantía. En todos los niveles de garantía, el producto, servicio o proceso de TIC debe contener varias funciones de seguridad, definidas por el esquema, 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 tanto de pila (*stack*) como de almacenamiento libre o dinámico (*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 programas informáticos como equipos informáticos.

(88) 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, servicio o proceso 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 un servicio de TIC. En los casos en que un esquema europeo de certificación de la ciberseguridad establezca una autoevaluación de la conformidad, debe ser suficiente con que el fabricante o proveedor de los productos, servicios o procesos de TIC haya llevado a cabo una autoevaluación sobre el cumplimiento de los procesos, productos o servicios de TIC con respecto al esquema de certificación.

(89) En el caso del nivel de garantía «sustancial», la evaluación, además de cumplir con lo indicado para el nivel de garantía «básico», debe regirse al menos por la verificación del cumplimiento de las funcionalidades de seguridad del producto, servicio o proceso de TIC con respecto a su documentación técnica.

(90) Para el nivel de garantía «elevado», la evaluación, además de cumplir con lo indicado para el nivel de garantía «sustancial», debe regirse al menos por una prueba de eficacia que evalúe la resistencia de las funcionalidades de seguridad del producto, servicio o proceso de TIC frente a ciberataques complejos efectuados por personas que tienen habilidades y recursos significativos.

(91) 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 disponga otra cosa en el Derecho de la Unión o en el Derecho de los Estados miembros adoptado con arreglo al Derecho de la Unión. Puesto que el Derecho no está armonizado, los Estados miembros deben poder adoptar reglamentos técnicos nacionales que establezcan la certificación obligatoria en virtud de un esquema europeo de certificación de la ciberseguridad de conformidad con la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([20]). Los Estados miembros también pueden recurrir a la certificación europea de la ciberseguridad en el contexto de la contratación pública y de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([21]).

(92) Para mejorar el nivel de la ciberseguridad de algunos ámbitos en la Unión Europea, en el futuro podría revelarse necesario convertir en obligatorias para algunos productos, servicios o procesos de TIC, determinadas exigencias específicas en materia de ciberseguridad, así como la certificación relacionada con ella. La Comisión debe realizar de forma periódica un seguimiento de la incidencia de los esquemas de certificación adoptados sobre la disponibilidad en el mercado interior de productos, servicios y procesos de TIC seguros y evaluar periódicamente el grado de utilización de los esquemas de certificación para los fabricantes y proveedores de productos, servicios y procesos de TIC en la Unión. Sería conveniente analizar la eficacia de los esquemas europeos de certificación de la ciberseguridad y si determinados esquemas deben convertirse en obligatorios a la luz de la legislación de la Unión relativa a la ciberseguridad, en particular la Directiva (UE) 2016/1148, teniendo en cuenta la seguridad de las redes y los sistemas de información utilizados por los operadores de servicios esenciales.

(93) Los certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE deben ayudar a los usuarios finales a elegir con conocimiento de causa. Así pues, los productos, servicios y procesos de TIC que han sido certificados o para los que se ha expedido una declaración de conformidad de la UE deben ir acompañados de información estructurada, adaptada al nivel técnico previsto del usuario al que se destinan. Toda la información debe estar disponible en línea, y cuando proceda, podría estar disponible en formato físico. El usuario final debe poder tener acceso a informaciones relativas al número de referencia del esquema de certificación, al nivel de garantía, a la descripción de riesgos relacionados con la ciberseguridad asociados al producto, servicio o proceso de TIC, a la autoridad u organismo emisor, o debe poder obtener una copia del certificado europeo de ciberseguridad. Además, debe informarse al usuario final sobre la política de apoyo a la ciberseguridad (es decir, durante cuánto tiempo podrá el usuario final esperar recibir actualizaciones y correcciones de la ciberseguridad) del fabricante o del proveedor de productos, servicios o procesos de TIC. Cuando proceda, debe recibir orientaciones sobre las acciones o los ajustes que el usuario final podrá ejecutar para mantener o aumentar la ciberseguridad de productos, servicios o procesos de TIC, y ser informado sobre un punto de contacto único para comunicarse y recibir apoyo en caso de ciberataques (además de la comunicación automática). Dicha información debe actualizarse periódicamente y estar disponible en un sitio web que facilite información sobre los esquemas europeos de certificación de la ciberseguridad.

(94) Con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los esquemas o procedimientos nacionales de certificación de la ciberseguridad para productos, servicios o procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de una fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos esquemas nacionales de certificación de la ciberseguridad para productos, servicios o procesos de TIC cubiertos ya por un esquema europeo de certificación de la ciberseguridad existente. No obstante, no debe impedirse a los Estados miembros adoptar o conservar esquemas nacionales de certificación de la ciberseguridad con fines de seguridad nacional. Los Estados miembros deben comunicar a la Comisión y al GECC su intención de introducir nuevos esquemas nacionales de certificación de la ciberseguridad. La Comisión y el GECC deben evaluar el impacto del nuevo esquema nacional de certificación de la ciberseguridad sobre el correcto funcionamiento del mercado interior, y ponderar el posible interés estratégico de solicitar en su lugar un esquema europeo de certificación de la ciberseguridad.

(95) Los esquemas europeos de certificación de la ciberseguridad están destinados a ayudar a la armonización de las prácticas de ciberseguridad dentro de la Unión. Han de contribuir a aumentar el nivel de seguridad en el seno de la Unión. Además, cuando se conciban estos esquemas debe tenerse en cuenta y permitirse la introducción de innovaciones en materia de ciberseguridad.

([20]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (Texto pertinente a efectos del EEE) (DO L 241 de 17.9.2015, p. 1).

([21]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

(96) Los esquemas europeos de certificación de la ciberseguridad deben tener en cuenta los métodos actuales de desarrollo de programas informáticos y sus correspondientes equipos y, en especial, el impacto de las frecuentes actualizaciones de los programas informáticos o de los microprogramas incorporados sobre los certificados europeos de la ciberseguridad individuales. Los esquemas europeos de certificación de la ciberseguridad deben especificar las condiciones en que una actualización podrá exigir que un producto, servicio o proceso de TIC tenga que volver a ser certificado o que se reduzca el ámbito de un certificado europeo de la ciberseguridad específico, teniendo en cuenta cualquier posible efecto negativo de la actualización sobre la conformidad con los requisitos de seguridad del certificado.

(97) Una vez que se adopte un esquema europeo de certificación de la ciberseguridad, los fabricantes o proveedores de productos, servicios o procesos de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios de TIC al organismo de evaluación de la conformidad que prefieran en cualquier parte de la Unión. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo nacional de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y debe renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos nacionales 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.

(98) Las referencias en la legislación nacional a normas nacionales que hayan dejado de producir efectos jurídicos debido a la entrada en vigor de un esquema europeo de certificación de la ciberseguridad pueden ser una fuente de confusión. Por consiguiente, los Estados miembros deben reflejar en sus legislaciones nacionales la adopción de un esquema europeo de certificación de la ciberseguridad.

(99) Para conseguir una equivalencia normativa en toda la Unión, facilitar el reconocimiento mutuo y favorecer la aceptación global de los certificados europeos de la ciberseguridad y declaraciones de conformidad de la UE, es necesario poner a punto un sistema de evaluación interpares entre las autoridades nacionales de certificación de la ciberseguridad. Dicha evaluación interpares debe abarcar la conformidad de los procedimientos de supervisión de los productos, servicios y procesos de TIC con los correspondientes certificados europeos de la ciberseguridad, de vigilancia del respeto de las obligaciones de los fabricantes o de los proveedores de los productos, servicios y procesos de TIC que realizan una autoevaluación de la conformidad y de vigilancia de la conformidad de los organismos de evaluación, así como la adecuación de los conocimientos especializados del personal de los organismos que expiden los certificados para niveles de garantía «elevados». La Comisión, mediante un acto de ejecución, debe poder establecer al menos un plan quinquenal para la evaluación interpares, además de fijar los criterios y métodos de funcionamiento de dicho sistema de evaluación interpares.

(100) Sin perjuicio del sistema general de evaluación interpares que se establezca entre todas las autoridades nacionales de certificación de la ciberseguridad en relación con el marco de certificación europea de la ciberseguridad, determinados esquemas de certificación europea de la ciberseguridad pueden incluir un mecanismo de evaluación interpares para aquellos organismos que expidan certificados europeos de ciberseguridad de los productos, servicios y procesos de TIC con un nivel de garantía «elevado» en aplicación de dichos esquemas. El GECC debe apoyar la aplicación de dichos mecanismos de evaluación interpares. Dichas evaluaciones interpares deben establecer en particular si los organismos de que se trate desempeñan sus cometidos de forma armonizada y pueden incluir vías de recurso. Los resultados de las evaluaciones interpares deben hacerse públicos. Estos organismos pueden adoptar las medidas apropiadas para adaptar sus prácticas y sus conocimientos especializados en consecuencia.

(101) Los Estados miembros deben designar a una o más autoridades nacionales de certificación de la ciberseguridad para supervisar el cumplimiento de las obligaciones derivadas del presente Reglamento. Una autoridad nacional de certificación de la ciberseguridad puede ser una existente o una nueva autoridad. Asimismo, un Estado miembro debe poder designar, previo acuerdo con otro Estado miembro, a una o más autoridades nacionales de certificación de la ciberseguridad en el territorio de ese otro Estado miembro.

(102) En particular, las autoridades nacionales de certificación de la ciberseguridad deben supervisar y hacer cumplir las obligaciones de los fabricantes o proveedores de productos, servicios o procesos 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 esquema europeo de certificación de la ciberseguridad y hacer el seguimiento de la correspondiente evolución 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 europeos de la ciberseguridad expedidos por ellas o en relación con los certificados europeos de la ciberseguridad expedidos por los organismos de evaluación de la conformidad, cuando dichos certificados se refieran al nivel de garantía «elevado», deben 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, las autoridades nacionales de certificación de la ciberseguridad 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, servicios y procesos de TIC que no se ajusten a los requisitos del presente Reglamento o de esquemas europeos de certificación de la ciberseguridad específicos. La Comisión debe facilitar ese intercambio de información poniendo a disposición un sistema electrónico general de apoyo a la información, por ejemplo, el sistema de información y comunicación para la vigilancia del mercado (siglas inglesas ICSMS) o el sistema de alerta rápida para productos peligrosos no alimenticios (RAPEX), ya utilizados por las autoridades de vigilancia del mercado en virtud del Reglamento (CE) n.º 765/2008.

(103) Con vistas a garantizar la aplicación coherente del marco europeo de certificación de la ciberseguridad, debe establecerse un GECC, constituido por representantes de las autoridades nacionales de certificación de la ciberseguridad u otras autoridades nacionales pertinentes. Los cometidos principales del GECC 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 ENISA en la preparación de las propuestas de esquemas de certificación de la ciberseguridad, en casos debidamente justificados solicitar a ENISA que prepare una propuesta de esquema, y adoptar dictámenes dirigidos a ENISA sobre propuestas de esquemas y adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los esquemas europeos de certificación de la ciberseguridad existentes. El GECC debe facilitar el intercambio de buenas prácticas y conocimientos especializados entre las diferentes autoridades nacionales de certificación de la ciberseguridad responsables de la autorización de los organismos de evaluación de la conformidad y la expedición de certificados europeos de la ciberseguridad.

(104) Con el fin de reforzar la sensibilización y facilitar la aceptación de los futuros esquemas europeos de certificación de ciberseguridad, la Comisión 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, servicios y procesos TIC certificados.

(105) 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 Tratado de Funcionamiento de la Unión Europea (TFUE), puede celebrar acuerdos de reconocimiento mutuo relativos a certificados europeos de ciberseguridad. La Comisión, teniendo en cuenta el asesoramiento de ENISA y del GECC, puede recomendar que se inicien las negociaciones correspondientes. Cada esquema europeo de certificación de la ciberseguridad debe proporcionar condiciones específicas para dichos acuerdos de reconocimiento mutuo con terceros países.

(106) A fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([22]).

(107) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los esquemas europeos de certificación de la ciberseguridad de productos, servicios o procesos de TIC, para la adopción de los actos de ejecución sobre las disposiciones de ejecución de las investigaciones por parte de ENISA; para la adopción de los actos de ejecución sobre un plan para la revisión interpares de las autoridades nacionales de certificación de la ciberseguridad y para la adopción de los actos de ejecución 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.

(108) Las actividades de ENISA deben evaluarse de modo periódico e independiente. La evaluación debe tener en cuenta el logro de sus objetivos por parte de ENISA, sus prácticas de trabajo y la pertinencia de sus tareas, en particular sus tareas relativas a la cooperación operativa a nivel de la Unión. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad. En caso de procederse a una revisión, la Comisión debe evaluar el modo de reforzar el papel de ENISA como punto de referencia en materia de asesoramiento y conocimiento especializado y debe también evaluar que se encomiende a ENISA el cometido de apoyar la evaluación de los productos, servicios y procesos de TIC de terceros países que no cumplan las normas de la Unión, cuando dichos productos, servicios y procesos entren en la Unión.

([22]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(109) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, pueden lograrse mejor a escala 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 (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

(110) Procede derogar el Reglamento (UE) n.º 526/2013.

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 alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, el presente Reglamento establece:

a) los objetivos, tareas y aspectos organizativos relativos a ENISA (Agencia de la Unión Europea para la Ciberseguridad), y

b) un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

El marco a que se refiere el párrafo primero, letra b), se aplicará sin perjuicio de las disposiciones específicas contenidas en otros actos jurídicos de la Unión relativas a la certificación de carácter voluntario u obligatorio.

2. El presente Reglamento se entenderá sin perjuicio de las competencias de los Estados miembros en materia de 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 los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas;

2) «redes y sistemas de información»: las redes y sistemas de información según se definen en el artículo 4, punto 1, de la Directiva (UE) 2016/1148;

3) «estrategia nacional de seguridad de las redes y sistemas de información»: una estrategia nacional de seguridad de las redes y sistemas de información según se define en el artículo 4, punto 3, de la Directiva (UE) 2016/1148;

4) «operador de servicios esenciales»: un operador de servicios esenciales según se define en el artículo 4, punto 4, de la Directiva (UE) 2016/1148;

5) «proveedor de servicios digitales»: un proveedor de servicios digitales según se define en el artículo 4, punto 6, de la Directiva (UE) 2016/1148;

6) «incidente»: un incidente según se define en el artículo 4, punto 7, de la Directiva (UE) 2016/1148;

7) «gestión de incidentes»: la gestión de incidentes según se define en el artículo 4, punto 8, de la Directiva (UE) 2016/1148;

8) «ciberamenaza»: cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas;

9) «esquema europeo de certificación de la ciberseguridad»: conjunto completo, de disposiciones, requisitos técnicos, normas y procedimientos establecidos a escala de la Unión y que se aplican a la certificación o a la evaluación de la conformidad de los productos, servicios y procesos de TIC específicos;

10) «esquema nacional de certificación de la ciberseguridad»: conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos desarrollados y adoptados por una autoridad pública nacional, y que se aplican a la certificación o a la evaluación de la conformidad de los productos, servicios y procesos de TIC incluidos en el ámbito de aplicación de dicho esquema específico;

11) «certificado europeo de ciberseguridad»: documento expedido por el organismo pertinente que certifica que determinado, producto, servicio o proceso de TIC ha sido evaluado para verificar que cumple los requisitos específicos de seguridad establecidos en un esquema europeo de certificación de la ciberseguridad;

12) «producto de TIC»: un elemento o un grupo de elementos de las redes y los sistemas de información;

13) «servicio de TIC»: un servicio que consista, en su totalidad o principalmente, en la transmisión, almacenamiento, extracción o tratamiento de información mediante redes y sistemas de información;

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

15) «acreditación»: una acreditación tal como se define en el artículo 2, punto 10, del Reglamento (CE) n.º 765/2008;

16) «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;

17) «evaluación de la conformidad»: una evaluación de la conformidad tal como se define en el artículo 2, punto 12, del Reglamento (CE) n.º 765/2008;

18) «organismo de evaluación de la conformidad»: un organismo de evaluación de la conformidad tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008;

19) «norma»: una norma según se define en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012;

20) «especificación técnica»: un documento que prescribe los requisitos técnicos que debe cumplir un producto, servicio o proceso de TIC, o procedimientos de evaluación de la conformidad relativos a los mismos;

21) «nivel de garantía»: un fundamento que permite garantizar que un producto, servicio o proceso de TIC cumple los requisitos de seguridad de un esquema europeo específico de certificación de la ciberseguridad, indica el nivel en el que se ha evaluado el producto, servicio o proceso de TIC pero no mide la seguridad de un producto, servicio o proceso de TIC en sí mismo;

22) «autoevaluación de la conformidad»: una acción realizada por un fabricante o un proveedor de productos, servicios o procesos de TIC que evalúa el cumplimiento por estos de los requisitos establecidos en el esquema europeo de certificación de la ciberseguridad específico.

TÍTULO II

ENISA (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD)

CAPÍTULO I

Mandato y objetivos

Artículo 3

Mandato

1. ENISA desempeñará el cometido que le asigna el presente Reglamento con el fin de lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros, a las instituciones, órganos y organismos de la Unión en la mejora de la ciberseguridad. ENISA actuará como punto de referencia de asesoramiento y conocimientos especializados en cuestiones relacionadas con la ciberseguridad para las instituciones, órganos y organismos de la Unión, así como para otras partes interesadas pertinentes de la Unión.

Al desempeñar las tareas que le asigna el presente Reglamento, ENISA contribuirá a reducir la fragmentación del mercado interior.

2. ENISA desempeñará los cometidos que le confieran los actos jurídicos de la Unión que establecen medidas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de ciberseguridad.

3. Al desempeñar sus funciones, ENISA actuará con independencia, evitando la duplicación con las actividades de los Estados miembros y teniendo en cuenta los conocimientos ya existentes de los Estados miembros.

4. ENISA desarrollará sus recursos propios, en particular las capacidades y las competencias humanas y técnicas, necesarios para desarrollar las tareas que le asigna el presente Reglamento.

Artículo 4

Objetivos

1. ENISA 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. ENISA 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. ENISA prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a las instituciones, órganos y organismos de la Unión, 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. ENISA fomentará la cooperación, en particular el intercambio de información, 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. ENISA contribuirá a incrementar las capacidades de ciberseguridad a nivel de la Unión para apoyar las acciones de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

6. ENISA promoverá el uso de la certificación europea de ciberseguridad, con vistas a evitar la fragmentación del mercado interior. ENISA contribuirá a la creación y al mantenimiento de un marco de certificación europea de la ciberseguridad de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos, servicios y procesos de TIC y reforzar así la confianza en el mercado interior digital y su competitividad.

7. ENISA promoverá un alto nivel de sensibilización sobre ciberseguridad, en particular ciberhigiene y ciberalfabetización de los ciudadanos, organizaciones y empresas.

CAPÍTULO II

Tareas

Artículo 5

Elaboración y ejecución de la política y del Derecho de la Unión

ENISA contribuirá a la elaboración y ejecución de la política y del Derecho de la Unión:

1. Prestando asistencia y asesoramiento, en la elaboración y la revisión de la política y del Derecho 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 en particular emitiendo su dictamen y sus análisis independientes y aportando trabajos preparatorios.

2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y el Derecho 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 el compartir información, así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto.

3. Asistiendo a los Estados miembros y a las instituciones, órganos y organismos de la Unión para que elaboren y promuevan políticas de ciberseguridad que apoyen la disponibilidad general y la integridad del núcleo público de la internet abierta.

4. Contribuyendo a los trabajos del Grupo de cooperación con arreglo al artículo 11 de la Directiva (UE) 2016/1148, ofreciendo su asesoramiento y asistencia.

5. Respaldando:

   a) la elaboración y la ejecución 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;

   b) 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;

   c) la asistencia a los Estados miembros en la ejecución de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de los datos y la privacidad, así como la emisión, previa solicitud, de un dictamen para el Comité Europeo de Protección de Datos.

6. 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 informaciones sobre las notificaciones de incidentes de los Estados miembros transmitidas 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) el resumen de las notificaciones de violación de la seguridad y pérdida de la integridad respecto de los proveedores de servicios de confianza, transmitidas por los organismos de supervisión a ENISA, de conformidad con el artículo 19, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([23]);

   c) las notificaciones de incidentes relacionados con la seguridad transmitidas por los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, transmitidas por las autoridades competentes a ENISA, de conformidad con el artículo 40 de la Directiva (UE) 2018/1972.

([23]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

Artículo 6

Creación de capacidades

1. ENISA asistirá:

a) a los Estados miembros en sus esfuerzos por mejorar la prevención, detección, análisis y capacidad de respuesta a ciberamenazas e incidentes, proporcionándoles los conocimientos teóricos y prácticos;

b) con carácter voluntario, a los Estados miembros y las instituciones, órganos y organismos de la Unión en el establecimiento y la aplicación de políticas de divulgación de vulnerabilidades;

c) a las instituciones, órganos y organismos de la Unión en sus esfuerzos para mejorar la prevención, detección, análisis de ciberamenazas e incidentes y para mejorar su capacidad de respuesta a dichas ciberamenazas e incidentes, en particular a través de un apoyo adecuado al CERT;

d) a los Estados miembros, a petición suya, en el desarrollo de CSIRT nacionales, con arreglo al artículo 9, apartado 5, de la Directiva (UE) 2016/1148;

e) 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, y también promoverá la difusión y tomará nota de los progresos en la aplicación de estas estrategias en toda la Unión, con el fin de promover las mejores prácticas;

f) 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;

g) 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;

h) a los Estados miembros, organizando periódicamente ejercicios de ciberseguridad a escala de la Unión a que se refiere el artículo 7, apartado 5, y ello al menos cada dos años, y formulando recomendaciones políticas basadas en el proceso de evaluación de los ejercicios y en las enseñanzas extraídas de ellos;

i) a los organismos públicos pertinentes, ofreciendo formación sobre ciberseguridad, en colaboración, cuando proceda, con las partes interesadas;

j) 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, en virtud del artículo 11, apartado 3, letra l), de la Directiva (UE) 2016/1148, incluso en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes.

2. ENISA 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. ENISA apoyará la cooperación operativa entre los Estados miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas.

2. ENISA 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 de disposiciones prácticas para la ejecución de tareas específicas previa consulta a la Comisión.

3. ENISA 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 apoyará activamente el intercambio de información y la cooperación entre sus miembros.

4. ENISA apoyará a los Estados miembros en lo relativo a la cooperación operativa dentro de la red de CSIRT:

a) asesorando sobre cómo mejorar su capacidad para prevenir, detectar y dar respuesta a los incidentes y, previa solicitud de uno o varios Estados miembros, proporcionando asesoramiento sobre una amenaza específica;

b) prestando asistencia, previa solicitud de uno o varios Estados miembros, en la evaluación de los incidentes con un impacto significativo o sustancial, proporcionando conocimientos técnicos y facilitando la gestión técnica de dichos incidentes, en particular apoyando el intercambio voluntario de información pertinente y soluciones técnicas entre Estados miembros;

c) analizando las vulnerabilidades e incidentes sobre la base de la información públicamente disponible o la información que los Estados miembros faciliten voluntariamente para este fin, y

d) previa solicitud de uno o varios Estados miembros, dando apoyo en las investigaciones técnicas *ex post* de los incidentes que tengan un impacto significativo o sustancial en el sentido de la Directiva (UE) 2016/1148.

En el desempeño de estas tareas, ENISA y el CERT-UE entablarán una cooperación estructurada con el fin de beneficiarse de las sinergias y evitar la duplicación de actividades.

5. ENISA 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 Unión en la organización de ejercicios de ciberseguridad a petición suya. Dichos ejercicios de ciberseguridad a nivel de la Unión podrán constar de elementos técnicos, operativos o estratégicos. Cada dos años, ENISA organizará un ejercicio global a gran escala.

En su caso, ENISA participará asimismo en la realización de ejercicios sectoriales de ciberseguridad, y contribuirá a organizarlos cuando proceda, junto con organizaciones competentes que también participen en los ejercicios de ciberseguridad a escala de la Unión.

6. ENISA, en estrecha colaboración con los Estados miembros, elaborará un informe periódico y detallado sobre la situación técnica de la ciberseguridad en la UE, relativo a incidentes y ciberamenazas, basándose en la información disponible al público, 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 (UE) 2016/1148, ambos con carácter voluntario; el EC3 y el CERT-UE.

7. ENISA contribuirá a la elaboración de una respuesta cooperativa, a nivel de la Unión y de los Estados miembros, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad, principalmente por los siguientes medios:

a) agregación y análisis de los informes procedentes de fuentes nacionales que son de dominio público y han sido 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) facilitación, previa petición, de la gestión técnica de tales incidentes 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 Unión y, previa petición, a los Estados miembros en la comunicación pública en torno a esos incidentes o crisis;

e) prueba de los planes de cooperación para responder a dichos incidentes o crisis a nivel de la Unión y apoyo, previa petición, a los Estados miembros para que prueben dichos planes a escala nacional.

Artículo 8

Mercado, certificación de la ciberseguridad y normalización

1. ENISA apoyará y promoverá el desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de, productos, servicios y procesos de TIC, según lo establecido en el título III del presente Reglamento, por los siguientes medios:

a) controlar permanentemente los avances en los ámbitos de normalización relacionados y recomendar unas especificaciones técnicas apropiadas que se puedan utilizar en el desarrollo de los esquemas europeos de certificación de la ciberseguridad mencionados en el artículo 54, apartado 1, letra c), cuando no se disponga de normas;

b) preparar propuestas de esquemas europeos de certificación de la ciberseguridad (en lo sucesivo, «propuestas de esquemas») para productos, servicios y procesos de TIC de conformidad con el artículo 49;

c) evaluar los esquemas europeos de certificación de la ciberseguridad adoptados de conformidad con el artículo 49, apartado 8;

d) participar en las revisiones interpares de conformidad con el artículo 59, apartado 4;

e) asistir a la Comisión, encargándose de la secretaría del GECC de conformidad con el artículo 62, apartado 5;

2. ENISA se encargará de la secretaría del Grupo de las Partes Interesadas de Certificación de la Ciberseguridad de conformidad con el artículo 22, del apartado 4.

3. ENISA recopilará y publicará directrices y desarrollar buenas prácticas, relativas a los requisitos de ciberseguridad de los productos, servicios y procesos de TIC, en cooperación con las autoridades nacionales de certificación de la ciberseguridad y con la industria, de una manera formal, estructurada y transparente.

4. ENISA contribuirá a un refuerzo de capacidades relacionada con los procesos de evaluación y certificación, recopilando y publicando directrices y proporcionando apoyo a los Estados miembros, a instancia de estos.

5. ENISA facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos, servicios y procesos de TIC.

6. ENISA elaborará, en colaboración con los Estados miembros y la industria, 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, en virtud del artículo 19, apartado 2, de la Directiva (UE) 2016/1148.

7. ENISA 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

ENISA:

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 ciberamenazas e incidentes con el fin de detectar las tendencias emergentes y ayudar a prevenir los incidentes;

c) en cooperación con los expertos de las autoridades de los Estados miembros y las partes interesadas pertinentes, emitirá dictámenes, orientaciones 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 de los sectores público y privado;

e) recopilará y analizará la información disponible públicamente relativa a incidentes significativos y elaborará informes con el fin de ofrecer orientaciones a los ciudadanos, organizaciones y empresas de toda la Unión.

Artículo 10

Sensibilización y educación

ENISA:

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

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

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 sensibilización y educación en materia de ciberseguridad.

Artículo 11

Investigación e innovación

En relación con la investigación y la innovación, ENISA:

a) asesorará a las instituciones, órganos y organismos de 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 ciberamenazas actuales y emergentes, 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;

c) contribuirá a la agenda estratégica de investigación e innovación a escala de la Unión en el ámbito de la ciberseguridad.

Artículo 12

Cooperación internacional

ENISA contribuirá a los esfuerzos de la Unión por cooperar con terceros países y organizaciones internacionales, así como dentro de los marcos de cooperación internacional pertinentes, a fin de promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad, por los siguientes medios:

a) participar, cuando proceda, como observador en la organización de ejercicios internacionales, y analizar los resultados de esos ejercicios e informar al respecto al Consejo de Administración;

b) facilitar, a petición de la Comisión, el intercambio de mejores prácticas;

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

d) facilitar asesoramiento y apoyo a la Comisión en materia de acuerdos de reconocimiento mutuo de certificados de ciberseguridad con terceros países en colaboración con el GECC creado en virtud del artículo 62.

CAPÍTULO III

Organización de ENISA

Artículo 13

Estructura de ENISA

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

a) un Consejo de Administración;

b) un Comité Ejecutivo;

c) un director ejecutivo;

d) un Grupo Consultivo de ENISA;

e) una red de funcionarios de enlace nacionales.

Sección 1

Consejo De Administración

Artículo 14

Composición del Consejo de Administración

1. El Consejo de Administración estará compuesto por un miembro nombrado por cada Estado miembro y dos miembros nombrados por la Comisión. Todos los miembros tendrán derecho a voto.

2. Cada miembro del Consejo de Administración tendrá un suplente. Dicho suplente representará al miembro 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 15

Funciones del Consejo de Administración

1. El Consejo de Administración:

a) definirá la orientación general del funcionamiento de ENISA 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 ENISA con las actividades realizadas por los Estados miembros y a nivel de la Unión;

b) adoptará el proyecto de documento único de programación de ENISA a que se refiere el artículo 24 antes de someterlo al dictamen de la Comisión;

c) adoptará, el documento único de programación de ENISA por una mayoría de dos tercios de sus miembros teniendo en cuenta el dictamen de la Comisión;

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

e) adoptará el presupuesto anual de ENISA y ejercerá otras funciones relacionadas con el presupuesto de ENISA de conformidad con el capítulo IV;

f) evaluará y adoptará el informe anual consolidado sobre las actividades de ENISA, que incluirá las cuentas y describirá en qué medida ENISA ha cumplido sus indicadores de rendimiento 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, y lo publicará;

g) adoptará las normas financieras aplicables a ENISA de conformidad con el artículo 32;

h) 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;

i) adoptará normas para la prevención y la gestión de los conflictos de intereses de sus miembros;

j) 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;

k) adoptará su propio reglamento interno, incluidas las normas relativas a las decisiones provisionales sobre la delegación de las tareas específicas con arreglo a lo dispuesto en el artículo 19, apartado 7;

l) ejercerá, respecto del personal de ENISA, las competencias atribuidas por el Estatuto de los funcionarios de la Unión Europea (en lo sucesivo, «Estatuto de los funcionarios») y las atribuidas por el Régimen aplicable a los otros agentes de la Unión Europea (en lo sucesivo, «Régimen aplicable a los otros agentes») establecidas por el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo ([24]) a la autoridad facultada para proceder a los nombramientos y a la autoridad facultada para proceder a las contrataciones (en lo sucesivo, «competencias de la autoridad facultada para proceder a los nombramientos») conforme al apartado 2;

m) adoptará las normas de aplicación del Estatuto de los funcionarios y del Régimen aplicable a los otros agentes, de conformidad con el procedimiento establecido en el artículo 110 de dicho Estatuto;

n nombrará al director ejecutivo y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 36;

o) nombrará a un contable, que podrá ser el contable de la Comisión, que será totalmente independiente en el desempeño de sus funciones;

p) adoptará todas las decisiones relativas al establecimiento de las estructuras internas de ENISA y, cuando sea necesario, a su modificación, teniendo en cuenta las necesidades de la actividad de ENISA, así como la buena gestión financiera;

q) autorizará el establecimiento de convenios de trabajo de conformidad en relación con el artículo 7;

r) autorizará el establecimiento y la celebración de convenios de trabajo de conformidad con el artículo 42.

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 podrá subdelegar esas competencias.

([24]) DO L 56 de 4.3.1968, p. 1.

3. Cuando así lo exijan circunstancias excepcionales, el Consejo de Administración podrá adoptar una decisión para 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 16

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. Su mandato será para un período de cuatro años, 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 17

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 Consultivo de ENISA 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 del Consejo de Administración por asesores o expertos, con sujeción al reglamento interno del Consejo de Administración.

6. ENISA se encargará de la secretaría del Consejo de Administración.

Artículo 18

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 el derecho a voto del miembro.

4. El presidente del Consejo de Administración 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 19

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 20, le asistirá y asesorará en la aplicación de las decisiones del Consejo de Administración en cuestiones administrativas y presupuestarias con arreglo al artículo 20.

3. El Comité Ejecutivo estará formado por cinco miembros. Los miembros del Comité Ejecutivo serán escogidos entre los miembros del Consejo de Administración. Uno de los miembros será el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y otro será uno de los representantes de la Comisión. Los nombramientos de los miembros del Comité Ejecutivo tratarán de alcanzar una representación de género equilibrada en el Comité Ejecutivo. 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 adicionales a petición de sus miembros.

6. El Consejo de Administración establecerá el reglamento interno del Comité Ejecutivo.

7. Cuando sea necesario, por motivos de urgencia, el Comité Ejecutivo podrá adoptar determinadas decisiones provisionales en nombre del Consejo de Administración, en particular en materia de gestión administrativa, incluida la suspensión de la delegación de las competencias atribuidas a la autoridad facultada para proceder a los nombramientos, y para cuestiones presupuestarias. Dichas decisiones provisionales serán comunicadas sin demora indebida al Consejo de Administración, que decidirá si la aprueba o la rechaza a más tardar tres meses después de que se haya tomado la decisión. El Comité Ejecutivo no tomará una decisión en nombre del Consejo de Administración que deba ser aprobada por una mayoría de dos tercios del Consejo de Administración.

Sección 3

Director Ejecutivo

Artículo 20

Funciones del director ejecutivo

1. ENISA 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 ENISA;

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 ENISA, 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 OLAF, y presentar informes sobre los progresos conseguidos, dos veces al año a la Comisión y periódicamente al Consejo de Administración;

h) preparar el proyecto de normas financieras aplicables a ENISA a que se refiere el artículo 32;

i) preparar el proyecto de estado de previsiones de ingresos y gastos de ENISA 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 ENISA y someterla a la aprobación del Consejo de Administración;

l) crear y mantener contactos con la comunidad empresarial y las organizaciones de consumidores para garantizar un diálogo continuado con las partes interesadas pertinentes;

m) intercambiar pareceres e información regularmente con las instituciones, órganos y organismos de la Unión sobre sus actividades en materia de ciberseguridad para garantizar la coherencia en la elaboración y ejecución de la política de la Unión;

n) desempeñar otros cometidos que el presente Reglamento le asigne.

4. Siempre que sea necesario y esté dentro del mandato de ENISA, 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. El director ejecutivo 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 ENISA.

5. Cuando sea necesario, con el fin de desempeñar las funciones de ENISA 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 miembro donde se encuentra la sede de ENISA, 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. El número agregado de efectivos en todas las oficinas locales se mantendrá en un mínimo y no superará el 40 % del total del personal de ENISA ubicado en el Estado miembro donde se encuentra la sede de ENISA. El número de efectivos en cada oficina local no superará el 10 % del total del personal de ENISA ubicado en el Estado miembro donde se encuentra la sede de ENISA.

Esta decisión especificará el alcance de las actividades que se llevarán a cabo en la oficina local, evitándose costes innecesarios y la duplicación de funciones administrativas de ENISA.

Sección 4

Grupo Consultivo de ENISA, Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad y red de funcionarios de enlace nacionales

Artículo 21

Grupo consultivo de ENISA

1. El Consejo de Administración establecerá de manera transparente, a propuesta del director ejecutivo, el Grupo Consultivo de ENISA compuesto 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, las pymes, los operadores de servicios esenciales, los grupos de consumidores, los expertos académicos en ciberseguridad y los representantes de las autoridades competentes notificadas de conformidad con la Directiva (UE) 2018/1972, las organizaciones europeas de normalización y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos. El Consejo de Administración velará por que haya una participación equilibrada entre hombres y mujeres y un equilibrio geográfico, así como un equilibrio entre los distintos grupos de partes interesadas.

2. Los procedimientos del Grupo Consultivo de ENISA, en particular con respecto a su composición, la propuesta por el director ejecutivo a que se refiere el apartado 1, el número y nombramiento de sus miembros y el funcionamiento del Grupo Consultivo ENISA, se especificarán en el reglamento operativo interno de ENISA y se harán públicos.

3. El Grupo Consultivo de ENISA estará presidido por el director ejecutivo o por cualquier otra persona que este designe en cada caso.

4. El mandato de los miembros del Grupo Consultivo de ENISA tendrá una duración de dos años y medio. Los miembros del Consejo de Administración no podrán ser miembros del Grupo Consultivo de ENISA. Los expertos de la Comisión y de los Estados miembros podrán asistir a las reuniones del Grupo Consultivo de ENISA y participar en sus trabajos. Se podrá invitar a asistir a las reuniones del Grupo Consultivo de ENISA y a participar en sus trabajos a representantes de otros órganos que no sean miembros del Grupo cuando el director ejecutivo lo considere pertinente.

5. El Grupo Consultivo de ENISA asesorará a ENISA en lo relativo a la realización de sus actividades, a excepción de la aplicación de las disposiciones del título III del presente Reglamento. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo anual de ENISA y en el mantenimiento de la comunicación con las partes interesadas pertinentes sobre los aspectos relativos al programa de trabajo.

6. El Grupo Consultivo de ENISA informará periódicamente al Consejo de Administración de sus actividades.

Artículo 22

Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad

1. Se establecerá el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad.

2. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad estará compuesto por miembros seleccionados de entre expertos reconocidos que representen a las partes interesadas pertinentes. La Comisión, tras una convocatoria transparente y abierta, seleccionará, con base en una propuesta de ENISA, a los miembros del Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad velando por una participación equilibrada entre distintos grupos de partes interesadas, así como entre hombres y mujeres y un equilibrio geográfico.

3. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad desempeñará las siguientes tareas:

a) asesorar a la Comisión sobre cuestiones estratégicas relativas al marco europeo de certificación de la ciberseguridad;

b) asesorar a ENISA, previa solicitud, sobre cuestiones generales y estratégicas relativas a los cometidos de ENISA en relación con el mercado, la certificación de la ciberseguridad y la normalización;

c) prestar asistencia a la Comisión en la elaboración del programa de trabajo evolutivo de la Unión previsto en el artículo 47;

d) emitir un dictamen sobre el programa de trabajo evolutivo de la Unión con arreglo al artículo 47, apartado 4, y

e) en situaciones urgentes, prestar asesoramiento a la Comisión y al GECC sobre la necesidad de contar con esquemas de certificación adicionales no incluidos en el programa de trabajo evolutivo de la Unión, según lo previsto en los artículos 47y 48.

4. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad estará copresidido por los representantes de la Comisión y de ENISA, y su secretaría correrá a cargo de ENISA.

Artículo 23

Red de funcionarios de enlace nacionales

1. El Consejo de Administración, a propuesta del director ejecutivo, establecerá una red de funcionarios de enlace nacionales, compuesta por representantes de todos los Estados miembros (en lo sucesivo, «funcionarios de enlace nacionales»). Cada Estado miembro nombrará a un representante de la Red de funcionarios de enlace nacionales.

Las reuniones de la red de funcionarios de enlace nacionales podrán celebrarse en distintas formaciones de expertos.

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

3. Los funcionarios de enlace nacionales actuarán como punto central de contacto a nivel nacional para facilitar la cooperación entre ENISA y los expertos nacionales en el contexto de la ejecución del programa de trabajo anual de ENISA.

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

5. Las funciones y los procedimientos de la red de funcionarios de enlace nacionales se especificarán en las normas internas de funcionamiento de ENISA y se harán públicos.

Sección 5

Funcionamiento

Artículo 24

Documento único de programación

1. ENISA 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 ([25]) y habida cuenta de 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, junto con cualquier versión posterior actualizada de dicho documento.

4. El documento único de programación será final tras la adopción definitiva del presupuesto general de la Unión y, en caso necesario, se adaptará en consecuencia.

([25]) 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).

5. El programa de trabajo anual incluirá objetivos detallados y los resultados esperados, incluidos los 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 de trabajo anual será coherente con el programa de trabajo plurianual a que se refiere el apartado 7. Indicará claramente qué tareas se han añadido, modificado o suprimido en relación con el ejercicio presupuestario anterior.

6. El Consejo de Administración modificará el programa de trabajo anual adoptado cuando se encomiende una nueva tarea a ENISA. 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, en particular 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 67.

Artículo 25

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 una 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. ENISA 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 26

Transparencia

1. ENISA llevará a cabo sus actividades con un alto grado de transparencia y de conformidad con el artículo 28.

2. ENISA 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 25.

3. El Consejo de Administración, a propuesta del director ejecutivo, podrá autorizar a cualesquiera partes interesadas a participar en calidad de observadores en algunas de las actividades de ENISA.

4. ENISA establecerá en sus normas internas de funcionamiento, las medidas prácticas de aplicación de las normas de transparencia a que se refieren los apartados 1 y 2.

Artículo 27

Confidencialidad

1. Sin perjuicio de lo dispuesto en el artículo 28, ENISA no divulgará a terceros la información que trate o reciba para la que se haya presentado una solicitud motivada de tratamiento confidencial.

2. Los miembros del Consejo de Administración, el director ejecutivo, los miembros del Grupo Consultivo de ENISA, los expertos externos que participen en los grupos de trabajo *ad hoc* y los miembros del personal de ENISA, incluidos los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal, respetarán la obligación de confidencialidad prevista en el artículo 339 del TFUE, incluso después de haber cesado en sus funciones.

3. ENISA establecerá en sus normas internas de funcionamiento 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 ENISA, el Consejo de Administración tomará la decisión de permitir a ENISA manejar información clasificada. En tal caso, ENISA, de común acuerdo con los servicios de la Comisión, adoptará unas normas de seguridad que aplique los principios de seguridad contenidos en las Decisiones (UE, Euratom) 2015/443 ([26]) y 2015/444 ([27]) de la Comisión. Dichas normas de seguridad incluirán, entre otras, disposiciones para el intercambio, tratamiento y almacenamiento de la información clasificada.

Artículo 28

Acceso a los documentos

1. El Reglamento (CE) n.º 1049/2001 se aplicará a los documentos en poder de ENISA.

2. El Consejo de Administración adoptará disposiciones para la aplicación del Reglamento (CE) n.º 1049/2001 a más tardar el 28 de diciembre de 2019.

3. Las decisiones tomadas por ENISA en virtud del artículo 8 del Reglamento (CE) n.º 1049/2001 podrán ser objeto de una reclamación ante el Defensor del Pueblo Europeo en virtud del artículo 228 del TFUE o de un recurso ante el Tribunal de Justicia de la Unión Europea en virtud del artículo 263 del TFUE.

CAPÍTULO IV

Establecimiento y estructura del presupuesto de ENISA

Artículo 29

Establecimiento del presupuesto de ENISA

1. El director ejecutivo elaborará cada año un proyecto de estado de previsiones de ingresos y gastos de ENISA 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 estado de previsiones un estado de previsiones de ingresos y gastos de ENISA para el siguiente ejercicio financiero.

3. El Consejo de Administración, a más tardar el 31 de enero de cada año, transmitirá el estado de previsiones, 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 42, apartado 2.

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

5. El Parlamento Europeo y el Consejo autorizarán los créditos necesarios para la contribución de la Unión destinada a ENISA.

6. El Parlamento Europeo y el Consejo adoptarán la plantilla de ENISA.

([26]) 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).

([27]) 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).

7. El Consejo de Administración adoptará el presupuesto de ENISA junto con el documento único de programación. El presupuesto de ENISA se convertirá en definitivo tras la adopción final del presupuesto general de la Unión Europea. Cuando proceda, el Consejo de Administración reajustará el presupuesto de ENISA y el documento único de programación con arreglo al presupuesto general de la Unión.

Artículo 30

Estructura del presupuesto de ENISA

1. Sin perjuicio de otros recursos, los ingresos de ENISA consistirán en:

a) una contribución procedente del presupuesto general de la Unión;

b) ingresos asignados a partidas de gastos específicas de conformidad con las normas financieras mencionadas en el artículo 32;

c) financiación de la Unión en forma de convenios de delegación o subvenciones *ad hoc*, de conformidad con las normas financieras mencionadas en el artículo 32 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 ENISA a que se refiere el artículo 42;

e) eventuales contribuciones voluntarias, dinerarias o en especie, de los Estados miembros.

Los Estados miembros que aporten contribuciones voluntarias en virtud del párrafo primero, letra e), no podrán reclamar ningún derecho o servicio específico como consecuencia de su contribución.

2. Los gastos de ENISA 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 31

Ejecución del presupuesto de ENISA

1. El director ejecutivo será responsable de la ejecución del presupuesto de ENISA.

2. El auditor interno de la Comisión ejercerá, con respecto a ENISA, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión.

3. El contable de ENISA remitirá las cuentas provisionales del ejercicio financiero (ejercicio N) al contable de la Comisión y al Tribunal de Cuentas a más tardar el 1 de marzo del ejercicio financiero siguiente (ejercicio N+1).

4. Tras recibir las observaciones formuladas por el Tribunal de Cuentas sobre las cuentas provisionales de ENISA, de conformidad con el artículo 246 del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo ([28]), el contable de ENISA elaborará las cuentas definitivas de ENISA bajo su responsabilidad y las presentará al Consejo de Administración para que este emita dictamen al respecto.

5. El Consejo de Administración emitirá un dictamen sobre las cuentas definitivas de ENISA.

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 de ENISA remitirá las cuentas definitivas de ENISA, juntamente con el dictamen del Consejo de Administración, al Parlamento Europeo, al Consejo, al contable de la Comisión y al Tribunal de Cuentas.

([28]) Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1).

8. En la misma fecha de transmisión de sus cuentas definitivas, el contable de ENISA 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 de ENISA en el *Diario Oficial de la Unión Europea* a más tardar el 15 de noviembre del año N + 1.

10. A más tardar el 30 de septiembre del año N + 1, el director ejecutivo remitirá al Tribunal de Cuentas una respuesta a sus observaciones, 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, de conformidad con el artículo 261, apartado 3, del Reglamento (UE, Euratom) 2018/1046.

12. El Parlamento Europeo, sobre la base de una recomendación del Consejo, deberá aprobar, antes del 15 de mayo del año N+ 2, la gestión del director ejecutivo respecto a la ejecución del presupuesto del año N.

Artículo 32

Normas financieras

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

Artículo 33

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 ([29]), ENISA, a más tardar el 28 de diciembre de 2019, suscribirá el Acuerdo Interinstitucional, de 25 de mayo de 1999, entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión de las Comunidades Europeas, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) ([30]), y adoptará las disposiciones apropiadas, que serán de aplicación a todo el personal de ENISA, sirviéndose del modelo contenido en el anexo de dicho Acuerdo.

2. El Tribunal de Cuentas tendrá la facultad de auditar, a partir de documentos e información obtenida a raíz de inspecciones *in situ*, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido de ENISA fondos de la Unión.

3. La OLAF podrá realizar investigaciones, incluidos controles y verificaciones sobre el terreno, de conformidad con las disposiciones y los procedimientos establecidos en el Reglamento n.º 883/2013 y el Reglamento (Euratom, CE) n.º 2185/96 ([31]) del Consejo, 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 ENISA.

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 ENISA, 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.

([29]) 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).

([30]) DO L 136 de 31.5.1999, p. 15.

([31]) 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).

CAPÍTULO V

Personal

Artículo 34

Disposiciones generales

El Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, así como las normas adoptadas de común acuerdo entre las instituciones de la Unión con el fin de poner en práctica el Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, se aplicarán al personal de ENISA.

Artículo 35

Privilegios e inmunidades

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

Artículo 36

Director ejecutivo

1. El director ejecutivo será contratado como agente temporal de ENISA 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, ENISA 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 diputados.

5. El mandato del director ejecutivo tendrá una duración de cinco años. Al final de ese período, la Comisión realizará una evaluación de la actuación del director ejecutivo y de las futuras tareas y desafíos de ENISA.

6. El Consejo de Administración se pronunciará sobre el nombramiento, la prórroga del mandato o el cese del director ejecutivo de conformidad con el artículo 18, apartado 2.

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 cinco años.

8. El Consejo de Administración informará al Parlamento Europeo acerca de su intención de prorrogar el mandato del director ejecutivo. En los tres meses que precedan a la prórroga de su mandato, el director ejecutivo hará, si se le invita a ello, una declaración ante la comisión pertinente del Parlamento Europeo y responderá a las preguntas formuladas por los parlamentarios.

9. Un director ejecutivo cuyo mandato haya sido prorrogado no podrá participar en otro procedimiento de selección para el mismo puesto.

10. El director ejecutivo solo podrá ser cesado por una decisión del Consejo de Administración, a propuesta de la Comisión.

Artículo 37

Expertos nacionales en comisión de servicios y otros agentes

1. ENISA podrá recurrir a expertos nacionales en comisión de servicios o a otro personal no contratado por ENISA. 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 ENISA.

CAPÍTULO VI

Disposiciones generales relativas a ENISA

Artículo 38

Estatuto jurídico de ENISA

1. ENISA será un órgano de la Unión dotado de personalidad jurídica.

2. En cada Estado miembro, ENISA disfrutará de la capacidad jurídica más amplia que se conceda a las personas jurídicas en el Derecho interno. En particular, podrá adquirir o vender propiedad mobiliaria e inmobiliaria y ser parte en actuaciones judiciales.

3. ENISA estará representada por su director ejecutivo.

Artículo 39

Responsabilidad de ENISA

1. La responsabilidad contractual de ENISA 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 ENISA.

3. En materia de responsabilidad extracontractual, ENISA 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 los daños a que se refiere el apartado 3.

5. La responsabilidad personal del personal de ENISA respecto a ENISA se regirá por las disposiciones pertinentes aplicables al personal de ENISA.

Artículo 40

Régimen lingüístico

1. El Reglamento n.º 1 del Consejo será aplicable a ENISA ([32]). Los Estados miembros y los demás organismos nombrados por los Estados miembros podrán dirigirse a ENISA 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 ENISA serán prestados por el Centro de traducción de los órganos de la Unión Europea.

Artículo 41

Protección de los datos de carácter personal

1. El tratamiento de los datos de carácter personal por parte de ENISA deberá ajustarse al Reglamento (UE) 2018/1725.

2. El Consejo de Administración adoptará las normas de ejecución a que se refiere el artículo 45, apartado 3, del Reglamento (UE) 2018/1725. El Consejo de Administración podrá adoptar otras medidas suplementarias necesarias para la aplicación del Reglamento (UE) 2018/1725 por parte de ENISA.

([32]) Reglamento n.º 1 por el que se fija el régimen lingüístico de la Comunidad Económica Europea (DO 17 de 6.10.1958, p. 385).

Artículo 42

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, ENISA podrá cooperar con las autoridades competentes de terceros países, con organizaciones internacionales, o con ambas. Para ello, ENISA podrá, previa aprobación de la Comisión, establecer acuerdos de trabajo con las autoridades de terceros países y organizaciones internacionales. Dichos acuerdos de trabajo no impondrán obligaciones jurídicas que incumban a la Unión y sus Estados miembros.

2. ENISA 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 de trabajo que precisen, en particular, el carácter, el alcance y las modalidades de participación de cada uno de estos países en la labor de ENISA, incluidas disposiciones sobre la participación en las iniciativas emprendidas por ENISA, las contribuciones financieras y el personal. Por lo que se refiere al personal, dichos mecanismos de trabajo serán, en cualquier caso, conformes con el Estatuto de los funcionarios y el Régimen aplicable a los otros agentes.

3. El Consejo de Administración adoptará una estrategia para las relaciones con terceros países u organizaciones internacionales en asuntos en los que sea competente ENISA. La Comisión velará por que ENISA opere dentro de su mandato y del marco institucional existente mediante la celebración de un convenio de trabajo adecuado con el director ejecutivo.

Artículo 43

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

Previa consulta a la Comisión, ENISA 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 sensible no clasificada y la ICUE, según lo dispuesto en las Decisiones (UE, Euratom) 2015/443 y 2015/444. Las normas de seguridad de ENISA incluirán disposiciones para el intercambio, tratamiento y almacenamiento de este tipo de información.

Artículo 44

Acuerdo relativo a la sede y condiciones de funcionamiento

1. Las disposiciones necesarias relativas al alojamiento que debe proporcionarse a ENISA en el Estado miembro de acogida y las instalaciones que debe poner a disposición dicho Estado miembro, así como las normas específicas aplicables en el Estado miembro de acogida al Director Ejecutivo, los miembros del Consejo de Administración, el personal de ENISA y los miembros de sus familias se establecerán en un acuerdo de sede entre ENISA y el Estado miembro donde se encuentre la sede, celebrado previa aprobación del Consejo de Administración.

2. El Estado miembro que acoja a ENISA ofrecerá las mejores condiciones posibles para garantizar su buen funcionamiento, teniendo en cuenta 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 de los miembros del personal.

Artículo 45

Control administrativo

El funcionamiento de ENISA 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 46

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 y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC.

2. El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas 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, dichos productos, servicios y procesos durante todo su ciclo de vida.

Artículo 47

Programa de trabajo evolutivo de la Unión para la certificación europea de la ciberseguridad

1. La Comisión publicará un programa de trabajo evolutivo para los esquemas europeos de certificación de la ciberseguridad (en lo sucesivo, «programa de trabajo evolutivo de la Unión») que definirá las prioridades estratégicas para los futuros esquemas europeos de certificación de la ciberseguridad.

2. El programa de trabajo evolutivo de la Unión incluirá en particular una lista de productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de la inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.

3. Se justificará la inclusión de un producto, servicio o proceso de TIC específico, o de categorías de los mismos, en un programa de trabajo evolutivo de la Unión, sobre la base de uno o más de los siguientes motivos:

a) la disponibilidad y el desarrollo de esquemas nacionales de certificación de la ciberseguridad que cubran cualquier categoría específica de productos, servicios o procesos de TIC y, en particular, en lo que se refiere al riesgo de fragmentación;

b) el Derecho o las políticas aplicables, de la Unión o de un Estado miembro;

c) la demanda del mercado;

d) la evolución del panorama de las ciberamenazas;

e) la solicitud de preparación de una propuesta de esquema específica por el GECC.

4. La Comisión tendrá debidamente en cuenta los dictámenes emitidos por el GECC y por el Grupo de las Partes Interesadas sobre Certificación del proyecto de programa de trabajo evolutivo de la Unión.

5. El primer programa de trabajo evolutivo de la Unión se publicará a más tardar el 10 de junio de 2020. El programa de trabajo evolutivo de la Unión se actualizará una vez cada tres años y más a menudo en caso necesario.

Artículo 48

Solicitud de un esquema europeo de certificación de la ciberseguridad

1. La Comisión podrá solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad existente basándose en el programa de trabajo evolutivo de la Unión.

2. En casos debidamente justificados, la Comisión o el GECC podrán solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad existente que no esté incluido en el programa de trabajo evolutivo de la Unión. El programa de trabajo evolutivo de la Unión se actualizará en consecuencia.

Artículo 49

Preparación, adopción y revisión de esquemas europeos de certificación de la ciberseguridad

1. Tras recibir una solicitud de la Comisión, con arreglo al artículo 48 ENISA preparará una propuesta de esquema que cumpla los requisitos establecidos en los artículos 51, 52 y 54.

2. Tras recibir una solicitud de la Comisión o del GECC con arreglo al artículo 48, apartado 2, ENISA podrá preparar una propuesta de esquema que cumpla los requisitos establecidos en los artículos 51, 52 y 54. Cuando ENISA rechace una solicitud, motivará su decisión. Toda decisión de rechazar dicha solicitud será adoptada por el Consejo de Administración.

3. A la hora de preparar las propuestas de esquema ENISA consultará a todas las partes interesadas mediante un proceso de consulta oficial transparente e inclusivo.

4. Para cada propuesta de esquema, ENISA creará un grupo *ad hoc* con arreglo al artículo 20, apartado 4, con el objetivo de facilitar a ENISA asesoramiento y conocimientos específicos.

5. ENISA cooperará estrechamente con el GECC. El GECC facilitará a ENISA la asistencia y el asesoramiento experto en relación con la preparación de la propuesta de esquema y adoptará un dictamen sobre la propuesta de esquema.

6. ENISA tomará en máxima consideración el dictamen del GECC antes de transmitir a la Comisión la propuesta de esquema preparada de conformidad con los apartados 3, 4 y 5. El dictamen del GECC no es vinculante para ENISA y su ausencia no impedirá a ENISA transmitir la propuesta de esquema a la Comisión.

7. La Comisión, a partir de la propuesta de esquema preparada por ENISA, podrá adoptar actos de ejecución que establezcan esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC que cumplan los requisitos de los artículos 51, 52 y 54. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 66, apartado 2.

8. ENISA evaluará al menos cada cinco años los esquemas europeos de certificación de la ciberseguridad teniendo en cuenta los comentarios recibidos de las partes interesadas. Si lo considera necesario, la Comisión o el GECC podrán pedir a ENISA que dé inicio al proceso de elaboración de una propuesta revisada de esquema conforme al artículo 48 y al presente artículo.

Artículo 50

Sitio web **de los esquemas europeos de certificación de la ciberseguridad**

1. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los esquemas europeos de certificación de la ciberseguridad, los certificados europeos de la ciberseguridad y las declaraciones UE de conformidad y darles publicidad, también en lo que se refiere a los esquemas europeos de certificación de la ciberseguridad que ya no son válidos y certificados europeos de la ciberseguridad y las declaraciones UE de conformidad retirados o caducados y al repositorio de hiperenlaces de información sobre ciberseguridad facilitado de conformidad con el artículo 55.

2. En su caso, el sitio web al que se refiere el apartado 1 indicará asimismo aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

Artículo 51

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

Los esquemas 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 tratados de otro modo frente al almacenamiento, tratamiento, acceso o revelación accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso de TIC;

b) proteger los datos almacenados, transmitidos o tratados de otro modo frente a la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso de TIC;

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) detectar y documentar las dependencias y vulnerabilidades conocidas;

e) registrar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;

f) que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;

g) verificar que los productos, servicios y procesos de TIC no contengan vulnerabilidades conocidas;

h) restaurar la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico;

i) que los productos, servicios y procesos de TIC sean seguros por defecto y desde el diseño;

j) que los productos, servicios y procesos de TIC se entreguen siempre con un programa informático y un equipo informático actualizados que no contengan vulnerabilidades conocidas públicamente, y dispongan de mecanismos para efectuar actualizaciones de seguridad.

Artículo 52

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

1. Un esquema europeo de certificación de la ciberseguridad podrá especificar uno o más de los niveles de garantía siguientes para los productos, servicios y procesos de TIC: «básico», «sustancial» o «elevado». El nivel de garantía deberá reflejar el nivel de riesgo asociado al uso previsto de un producto, servicio o proceso de TIC, en términos de probabilidad y repercusiones de un incidente.

2. Los certificados europeos de ciberseguridad o las declaraciones de conformidad de la UE mencionarán el nivel de garantía especificado en el esquema europeo de certificación de la ciberseguridad en el marco del cual ha sido expedido el certificado europeo de ciberseguridad o la declaración de conformidad de la UE.

3. Los requisitos de seguridad correspondientes a cada nivel de garantía se precisarán en el esquema europeo de certificación de la ciberseguridad pertinente, incluidas las funcionalidades de seguridad y el correspondiente rigor y profundidad necesarios para evaluar un producto, servicio o proceso de TIC.

4. El certificado o la declaración de la conformidad de la UE hará referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es reducir el riesgo de incidentes de ciberseguridad o evitarlos.

5. Un certificado europeo de ciberseguridad o una declaración de la conformidad de la UE que se refiere a un nivel de garantía «básico» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado o esa declaración de la conformidad cumplen los correspondientes 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 a efectuar incluirán al menos una revisión de la documentación técnica. Cuando dicha revisión no sea apropiada, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

6. Un certificado europeo de ciberseguridad que se refiere a un nivel de garantía «sustancial» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado cumplen los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos relacionados con la ciberseguridad conocidos, los riesgos de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados. Las actividades de evaluación a efectuar incluirán al menos: la revisión para demostrar la ausencia de las vulnerabilidades conocidas públicamente y la comprobación de que los productos, servicios o procesos de TIC aplican correctamente las funcionalidades de seguridad necesarias. Cuando dichas actividades de evaluación no sean apropiadas, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

7. Un certificado europeo de ciberseguridad que se refiere a un nivel de garantía «elevado» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado cumplen los correspondientes 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 a efectuar incluirán al menos: la revisión de la improcedencia de las vulnerabilidades conocidas públicamente, la comprobación de que los productos, procesos 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 pruebas de penetración. Cuando dichas actividades no sean apropiadas, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

8. Un esquema europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y la profundidad de los métodos 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 53

Autoevaluación de la conformidad

1. Un esquema europeo de certificación de la ciberseguridad podrá permitir realizar una autoevaluación de la conformidad bajo la responsabilidad exclusiva del fabricante o proveedor de productos, servicios o procesos de TIC. La autoevaluación de la conformidad únicamente se permitirá en relación con productos, servicios y procesos de TIC que presenten un bajo riesgo correspondientes al nivel de garantía «básico».

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

3. El fabricante o proveedor de productos, servicios o procesos de TIC deberá poner a disposición de la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 58, la declaración de conformidad de la UE, la documentación técnica y toda otra información pertinente relativa a la conformidad de los productos o servicios de TIC con un esquema durante el plazo previsto en el esquema europeo de certificación de la ciberseguridad correspondiente. Deberá presentarse a la autoridad nacional de certificación de la ciberseguridad y a ENISA una copia de la declaración de conformidad de la UE.

4. La expedición de una 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. Las declaraciones de conformidad de la UE serán reconocidas en todos los Estados miembros.

Artículo 54

Elementos de los esquemas europeos de certificación de la ciberseguridad

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

a) el objeto y alcance del esquema de certificación, incluido el tipo o categoría de productos, servicios y procesos de TIC cubiertos;

b) una descripción clara de la finalidad del esquema y de la manera en que las normas, los métodos de evaluación y los niveles de garantía seleccionados corresponden a las necesidades de los usuarios previstos del esquema;

c) referencias a las normas internacionales, europeas o nacionales que se han seguido para hacer la evaluación. En caso de que no haya normas disponibles, o de que estas no sean adecuadas, se deberá hacer referencia a las especificaciones técnicas que cumplen los requisitos del anexo II del Reglamento (UE) n.º 1025/2012 o, si no estuvieran disponibles, a las especificaciones técnicas o a otros requisitos de ciberseguridad definidos en el esquema europeo de certificación de la ciberseguridad;

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

e) una indicación de si está permitida, en virtud del esquema, la autoevaluación de la conformidad;

f) en su caso, requisitos específicos o adicionales a los que están sujetos los organismos de evaluación de la conformidad a fin de garantizar su capacidad técnica para evaluar los requisitos en materia de ciberseguridad;

g) los criterios y métodos de evaluación específicos que deben ser utilizados, incluidos los tipos de evaluación, para demostrar el logro de los objetivos de seguridad a que se refiere el artículo 51;

h) en su caso, la información necesaria para la certificación que un solicitante debe facilitar a los organismos de evaluación de la conformidad o poner a su disposición de otro modo;

i) cuando el esquema prevea marcas o etiquetas, las condiciones en las que pueden utilizarse tales marcas o etiquetas;

j) las normas para controlar el cumplimiento de los productos, servicios y procesos de TIC de los requisitos de los certificados europeos de ciberseguridad o de la declaración de conformidad de la UE, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

k) en su caso, condiciones para la expedición, el mantenimiento, la continuación y la renovación de un certificado europeo de ciberseguridad, así como condiciones para la ampliación o la reducción del alcance de la certificación;

l) las normas relativas a las consecuencias para los productos, servicios y procesos de TIC que han sido certificados o para los que se ha expedido una declaración de conformidad de la UE, pero que no cumplen con los requisitos del esquema;

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

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

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

p el contenido y formato de los certificados europeos de ciberseguridad y de la declaración de conformidad de la UE que van a ser expedidos;

q) el período de disponibilidad de la declaración de conformidad de la UE, la documentación técnica y toda otra información pertinente proporcionada por el fabricante o el proveedor de productos, servicios o procesos de TIC;

r) el período máximo de validez de los certificados europeos de ciberseguridad expedidos en virtud del esquema;

s) la política de divulgación para los certificados europeos de ciberseguridad expedidos, modificados o retirados en virtud del esquema;

t) las condiciones para el reconocimiento mutuo de los esquemas de certificación con terceros países;

u) en su caso, normas relativas a cualquier mecanismo de evaluación interpares establecido en el esquema respecto de las autoridades u organismos que expidan certificados europeos de ciberseguridad para niveles de garantía «elevados» con arreglo al artículo 56, apartado 6. Dicho mecanismo se entenderá sin perjuicio de las revisiones interpares previstas en el artículo 59;

v) formato y procedimientos que deben seguir los fabricantes y proveedores de productos, servicios o procesos de TIC para proporcionar y actualizar la información complementaria sobre ciberseguridad de conformidad con el artículo 55.

2. Los requisitos específicos del esquema europeo de certificación de la ciberseguridad serán coherentes con los requisitos legales aplicables, en particular los requisitos que emanen de las disposiciones armonizadas del Derecho de la Unión.

3. Cuando un acto jurídico específico de la Unión así lo prevea, podrá utilizarse la certificación o la declaración de conformidad de la UE en virtud de un esquema europeo de certificación de la ciberseguridad para demostrar la presunción de conformidad con los requisitos de dicho acto jurídico.

4. En ausencia de disposiciones armonizadas del Derecho de la Unión, el Derecho de un Estado miembro podrá prever también el uso de un esquema europeo de certificación de la ciberseguridad para establecer la presunción de conformidad con los requisitos legales.

Artículo 55

Información complementaria sobre ciberseguridad de productos, servicios y procesos de TIC certificados

1. El fabricante o proveedor de productos, servicios y procesos de TIC certificados o autoevaluados proporcionará la información sobre ciberseguridad complementaria siguiente:

a) orientaciones y recomendaciones para ayudar a los usuarios finales con la configuración, la instalación, el despliegue, el funcionamiento y el mantenimiento seguros de los productos o servicios de TIC;

b) el período durante el cual se ofrecerá a los usuarios finales apoyo en materia de seguridad, en particular en lo que se refiere a la disponibilidad de actualizaciones relacionadas con la ciberseguridad;

c) datos de contacto del fabricante o proveedor y métodos aceptados para recibir información sobre vulnerabilidad de usuarios finales o investigadores en materia de seguridad;

d) una referencia a los registros en línea en los que consten las vulnerabilidades conocidas públicamente en relación con el producto, servicio o proceso de TIC, así como recomendaciones pertinentes en materia de ciberseguridad.

2. La información a que se refiere el apartado 1 estará disponible en formato electrónico y seguirá estando disponible y siendo actualizada en función de las necesidades al menos hasta la expiración del correspondiente certificado europeo de ciberseguridad o de la declaración de conformidad de la UE.

Artículo 56

Certificación de la ciberseguridad

1. Los productos, servicios y procesos de TIC que hayan sido certificados de conformidad con un esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 49 se presumirán conformes con los requisitos de dicho esquema.

2. La certificación de la ciberseguridad será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros.

3. La Comisión evaluará periódicamente la eficacia y la utilización de los esquemas europeos de certificación de la ciberseguridad adoptados, así como si un esquema europeo de certificación de la ciberseguridad específico debe convertirse en obligatorio mediante el Derecho de la Unión aplicable para garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión y mejorar el funcionamiento del mercado interior. La primera de tales evaluaciones debe efectuarse a más tardar el 31 de diciembre de 2023, y las evaluaciones posteriores como mínimo cada dos años. La Comisión deberá, con base en los resultados de la evaluación, determinar los productos, servicios y procesos de TIC cubiertos por un esquema de certificación existente que deben estar cubiertos por un esquema de certificación obligatorio.

La Comisión atenderá, con carácter prioritario, a los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148, que se evaluarán a más tardar dos años después de la adopción del primer esquema europeo de certificación de la ciberseguridad.

Al preparar la evaluación, la Comisión deberá:

a) tener en cuenta las repercusiones de las medidas sobre los fabricantes o proveedores de dichos productos, servicios o procesos de TIC y sobre los usuarios en términos de costes, así como los beneficios sociales o económicos derivados del refuerzo previsto del nivel de seguridad de los productos, servicios y procesos de TIC de que se trate;

b) tener en cuenta la existencia y la aplicación del Derecho del Estado miembro y del tercer país pertinentes;

c) llevar a cabo un procedimiento de consulta abierto, transparente e inclusivo con todas las partes interesadas pertinentes y los Estados miembros;

d) tener en cuenta los plazos de aplicación, los períodos y medidas transitorios, en particular, respecto de las posibles repercusiones de la medida sobre los fabricantes o los proveedores de productos, servicios y procesos de TIC, incluidas las pymes;

e) proponer la manera más rápida y eficaz para llevar a cabo la transición entre un esquema de certificación voluntario y uno obligatorio.

4. Los organismos de evaluación de la conformidad a que se refiere el artículo 60 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 esquema europeo de certificación de la ciberseguridad adoptado por la Comisión de conformidad con el artículo 49.

5. No obstante lo dispuesto en el apartado 4, en casos debidamente justificados un esquema europeo de certificación de la ciberseguridad podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese esquema. Este organismo será uno de los siguientes:

a) una autoridad nacional de certificación de la ciberseguridad con arreglo al artículo 58, apartado 1, o

b) un organismo público que esté acreditado como organismo de evaluación de la conformidad con arreglo al artículo 60, apartado 1.

6. En los casos en que un esquema europeo de certificación de la ciberseguridad adoptado en virtud del artículo 49 requiera un nivel de garantía «elevado», el certificado europeo de ciberseguridad en virtud de dicho esquema solo podrá ser expedido por una autoridad nacional de certificación de la ciberseguridad o, en los siguientes casos, por un organismo de evaluación de la conformidad:

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

b) con base en una delegación general de la tarea de expedir tal certificado europeo de ciberseguridad por la autoridad nacional de certificación de la ciberseguridad a un organismo de evaluación de la conformidad.

7. La persona física o jurídica que presenta los productos, servicios o procesos de TIC para la certificación pondrá a disposición de la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 58, si dicha autoridad es el organismo que expide el certificado europeo de ciberseguridad, o del organismo de evaluación de la conformidad a que se refiere el artículo 60, toda la información necesaria para llevar a cabo el procedimiento de certificación.

8. El titular de un certificado europeo de ciberseguridad informará a la autoridad o al organismo a que se refiere el apartado 7, de cualquier vulnerabilidad o irregularidad que se detecte posteriormente, relativa a la seguridad del producto, servicio o proceso de TIC certificado, que pueda afectar al cumplimiento de los requisitos de certificación. La citada autoridad u organismo transmitirán dicha información sin demora indebida a la autoridad nacional de certificación de la ciberseguridad de que se trate.

9. Los certificados europeos de ciberseguridad se expedirán por el período previsto en el esquema europeo de certificación de la ciberseguridad y podrán renovarse siempre y cuando sigan cumpliéndose los requisitos correspondientes.

10. Los certificados europeos de ciberseguridad expedidos en virtud del presente artículo serán reconocidos en todos los Estados miembros.

Artículo 57

Esquemas y certificados nacionales de certificación de la ciberseguridad

1. Sin perjuicio de lo dispuesto en el apartado 3 del presente artículo, los esquemas nacionales de certificación de ciberseguridad y los procedimientos correspondientes para los productos, servicios y procesos de TIC cubiertos por un esquema 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 49, apartado 7. Los esquemas nacionales de certificación de la ciberseguridad y los procedimientos conexos para los productos, servicios y procesos de TIC que no estén cubiertos por un esquema europeo de certificación de la ciberseguridad seguirán existiendo.

2. Los Estados miembros se abstendrán de introducir nuevos esquemas nacionales de certificación de la ciberseguridad para productos, servicios y procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad en vigor.

3. Los certificados existentes expedidos de conformidad con esquemas nacionales de certificación de la ciberseguridad y cubiertos por un esquema europeo de certificación de la ciberseguridad seguirán siendo válidos hasta su fecha de caducidad.

4. Con vistas a evitar la fragmentación del mercado interior, los Estados miembros informarán a la Comisión y al GECC cualquier intención de crear nuevos esquemas nacionales de certificación de la ciberseguridad.

Artículo 58

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 nacionales de certificación de la ciberseguridad establecidas en ese otro Estado miembro para que se encarguen 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 nacionales de certificación de la ciberseguridad designadas. Cuando un Estado miembro designe más de una autoridad, también informará a la Comisión de las tareas que se hayan encomendado a cada una de dichas autoridades.

3. Sin perjuicio de lo establecido en el artículo 56, apartado 5), y en el artículo 56, apartado 6, 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.

4. Los Estados miembros se asegurarán de que las actividades de las autoridades nacionales de certificación de la ciberseguridad relacionadas con la expedición de certificados europeos de ciberseguridad de conformidad con el artículo 56, apartado 5, letra a), y el artículo 56, apartado 6, están estrictamente separadas de las actividades de supervisión establecidas en el presente artículo y de que dichas actividades se desempeñan de manera independiente una de la otra.

5. 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.

6. Para la aplicación eficaz del presente Reglamento, es conveniente que estas autoridades nacionales de certificación de la ciberseguridad participen en el GECC manera activa, eficaz, eficiente y segura.

7. Las autoridades nacionales de certificación de la ciberseguridad:

a) supervisarán y velarán por la aplicación de las normas recogidas en los esquemas europeos de certificación de la ciberseguridad en virtud del artículo 54, apartado 1, letra j), para controlar la conformidad de los productos, servicios y procesos de TIC con los requisitos de los certificados europeos de la ciberseguridad que hayan sido expedidos en sus respectivos territorios, en cooperación con otras autoridades de vigilancia del mercado pertinentes;

b) controlarán el cumplimiento y la aplicación de las obligaciones de los fabricantes y proveedores de productos, servicios o procesos de TIC establecidos en sus respectivos territorios y que llevan a cabo autoevaluaciones de la conformidad, en particular controlar el cumplimiento y la aplicación de las obligaciones de tales fabricantes y proveedores que figuran en el artículo 53, apartados 2 y 3, y en el correspondiente esquema europeo de certificación de la ciberseguridad;

c) sin perjuicio de lo dispuesto en el artículo 60, apartado 3, asistirán y apoyarán activamente 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;

d) controlarán y supervisarán las actividades de los organismos públicos mencionados en el artículo 56, apartado 5;

e) cuando proceda, autorizarán a los organismos de evaluación de la conformidad con arreglo al artículo 60, apartado 3, y restringirán, suspenderán o retirarán las autorizaciones en vigor en caso de incumplimiento, por parte de los organismos de evaluación de la conformidad, de los requisitos del presente Reglamento;

f) tramitarán las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados europeos de ciberseguridad expedidos por las autoridades nacionales de certificación de la ciberseguridad o los certificados europeos de ciberseguridad expedidos por los organismos de evaluación de la conformidad, de conformidad con el artículo 56, apartado 6, o en relación con las declaraciones de conformidad UE expedidas en virtud del artículo 53, 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;

g) presentarán a ENISA y al GECC un informe sucinto anual de las actividades realizadas con arreglo a las letras b), c) y d) del presente apartado y al apartado 8;

h) cooperarán con otras autoridades nacionales de certificación de la ciberseguridad u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos, servicios y procesos de TIC que no se ajusten a los requisitos del presente Reglamento o de esquemas europeos de certificación de la ciberseguridad específicos, y

i) seguirán las novedades de interés en el ámbito de la certificación de la ciberseguridad.

8. 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 presente 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 europeos de ciberseguridad y los responsables de expedir declaraciones de conformidad de la UE se ajustan al presente Reglamento o a un esquema 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 europeos de ciberseguridad expedidos por la autoridad nacional de certificación de la ciberseguridad o los certificados europeos de ciberseguridad expedidos por los organismos de evaluación de la conformidad, de conformidad con el artículo 56, apartado 6, que no se ajusten al presente Reglamento o a un esquema europeo de certificación de la ciberseguridad;

f) imponer sanciones conforme al Derecho nacional según lo establecido en el artículo 65, y solicitar el cese inmediato de la violación de las obligaciones establecidas en el presente Reglamento.

9. 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 productos, servicios y procesos de TIC.

Artículo 59

Revisión interpares

1. Con vistas a alcanzar normas equivalentes en toda la Unión en lo que respecta a los certificados europeos de ciberseguridad expedidos y a las declaraciones de conformidad de la UE, las autoridades nacionales de certificación de la ciberseguridad serán objeto de revisiones interpares.

2. La revisión interpares se llevará a cabo conforme a criterios y procedimientos de evaluación bien fundados y transparentes, en particular en lo relativo a los requisitos estructurales, de recursos humanos y de proceso, la confidencialidad y las reclamaciones.

3. La revisión interpares deberá evaluar:

a) cuando corresponda, si las actividades de la autoridad nacional de certificación de la ciberseguridad relacionadas con la expedición de certificados europeos de ciberseguridad a que se refiere el artículo 56, apartado 5, letra a), y el artículo 56, apartado 6, se acogen a una estricta separación de funciones y responsabilidades con respecto a las actividades de supervisión de conformidad con el artículo 58 y si ambas actividades funcionan de manera independiente;

b) los procedimientos de supervisión y cumplimiento de las normas para controlar la conformidad de los productos, servicios y procesos de TIC con los certificados, con arreglo al artículo 58, apartado 7;

c) los procedimientos de control y cumplimiento de las obligaciones de los fabricantes y proveedores de productos, servicios o procesos de TIC, de conformidad con el artículo 58, apartado 7, letra b);

d) los procedimientos de control, autorización y supervisión de las actividades de los organismos de evaluación de la conformidad;

e) cuando corresponda, si el personal de las autoridades u organismos que expiden certificados para un nivel de garantía «elevado» en virtud del artículo 56, apartado 6, tiene los conocimientos técnicos apropiados.

4. La revisión interpares será realizada, como mínimo cada cinco años, por al menos dos autoridades nacionales de certificación de la ciberseguridad de otros Estados miembros y por la Comisión. ENISA podrá participar en la revisión interpares.

5. La Comisión estará facultada para adoptar actos de ejecución mediante el establecimiento de un plan para las revisiones interpares que cubra un período de al menos cinco años y mediante la definición de los criterios relativos a la composición del equipo de revisión interpares, la metodología utilizada para la revisión, así como el calendario, la periodicidad y las demás tareas relativas a dicha revisión. A la hora de adoptar esos actos de ejecución, la Comisión tendrá debidamente en cuenta las observaciones del GECC.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 66, apartado 2.

6. El GECC analizará los resultados de la revisión interpares y redactará un resumen que se podrá hacer público y que formulará, cuando sea necesario, orientaciones o recomendaciones sobre las acciones o medidas que deban tomar las entidades afectadas.

Artículo 60

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. Dicha acreditación solamente se expedirá si se el organismo de evaluación de la conformidad cumple los requisitos establecidos en el anexo del presente Reglamento.

2. Cuando una autoridad nacional de certificación de la ciberseguridad expida un certificado europeo de ciberseguridad de conformidad con el artículo 56, apartado 5, letra a), y el artículo 56 apartado 6, 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.

3. Cuando los esquemas europeos de certificación de la ciberseguridad establezcan requisitos específicos o adicionales con arreglo al artículo 54, apartado 1, letra f), únicamente los organismos de evaluación de la conformidad a los que la autoridad nacional de certificación de la ciberseguridad haya autorizado por cumplir dichos requisitos podrán realizar tareas en el marco de dichos esquemas.

4. La acreditación mencionada en el apartado 1 se expedirá a los organismos de evaluación de la conformidad 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 nacionales de acreditación tomarán todas las medidas necesarias dentro de un período razonable de tiempo para restringir, suspender o revocar la acreditación de un organismo de evaluación de la conformidad expedida en virtud del apartado 1 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 61

Notificación

1. En relación con cada esquema europeo de certificación de la ciberseguridad adoptado, 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 60, apartado 3, para expedir certificados europeos de ciberseguridad de los niveles de garantía especificados en el artículo 52. Las autoridades nacionales de certificación de la ciberseguridad notificarán, sin dilaciones indebidas, cualquier modificación al respecto.

2. Un año después de la entrada en vigor de un esquema europeo de certificación de la ciberseguridad, la Comisión publicará en el *Diario Oficial de la Unión Europea* una lista de los organismos de evaluación de la conformidad notificados en virtud del citado esquema.

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 que se refiere el apartado 2 a un organismo de evaluación de la conformidad notificado por dicha autoridad. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de dicha 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 adoptar actos de ejecución para establecer 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 66, apartado 2.

Artículo 62

Grupo Europeo de Certificación de la Ciberseguridad

1. Queda establecido el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «GECC»).

2. El GECC estará integrado por representantes de las autoridades nacionales de certificación de la ciberseguridad o por representantes de otras autoridades nacionales pertinentes. Cualquier miembro del GECC tan solo podrá representar a otro Estado miembro.

3. Las partes interesadas y terceras partes podrán ser invitadas a asistir a las reuniones del GECC y a participar en sus trabajos.

4. El GECC 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 el programa de trabajo evolutivo de la Unión, las cuestiones de política de certificación de la ciberseguridad, la coordinación de los enfoques políticos y la preparación de los esquemas europeos de certificación de la ciberseguridad;

b) asistir, asesorar y cooperar con ENISA en relación con la preparación de una propuesta de esquema, de conformidad con el artículo 49;

c) adoptar un dictamen sobre la propuesta de esquema preparada por ENISA, de conformidad con el artículo 49;

d) solicitar a ENISA que prepare una propuesta de esquema de conformidad con el artículo 48, apartado 2;

e) adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los esquemas europeos de certificación de la ciberseguridad existentes;

f) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar información y buenas prácticas sobre los esquemas de certificación de la ciberseguridad;

g) 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;

h) proporcionar apoyo a la aplicación de los mecanismos de evaluación interpares según las normas establecidas en un esquema europeo de certificación de la ciberseguridad de conformidad con el artículo 54, apartado 1, letra u);

i) facilitar el alineamiento de los esquemas europeos de certificación de la ciberseguridad con las normas internacionales reconocidas, en particular mediante la revisión de los esquemas europeos de certificación de la ciberseguridad existentes y, cuando proceda, mediante la formulación de recomendaciones a ENISA para que colabore con las organizaciones internacionales de normalización correspondientes al objeto de solucionar las deficiencias o lagunas en las normas vigentes reconocidas a nivel internacional.

5. Con la asistencia de ENISA, la Comisión presidirá el GECC y se hará cargo de su secretaría, de conformidad con el artículo 8, apartado 1, letra e).

Artículo 63

Derecho a presentar una reclamación

1. Las personas físicas o jurídicas tendrán derecho a presentar una reclamación ante el responsable de expedir un certificado europeo de ciberseguridad o, cuando la reclamación esté relacionada con un certificado europeo de ciberseguridad expedido por un organismo de evaluación de la conformidad que actúe con arreglo al artículo 56, apartado 6, ante la autoridad nacional de certificación de la ciberseguridad pertinente.

2. La autoridad u organismo ante el que se haya presentado la reclamación informará al reclamante sobre el curso del procedimiento y la decisión tomada, e informará al reclamante sobre el derecho de recurso a la tutela judicial efectiva a que se refiere el artículo 64.

Artículo 64

Derecho a la tutela judicial efectiva

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva en lo que respecta a:

a) las decisiones de la autoridad u organismo mencionado en el artículo 63, apartado 1, en particular y cuando corresponda en lo que respecta a la expedición, la no expedición o el reconocimiento de un certificado europeo de ciberseguridad del que sea titular dicha persona física o jurídica;

b) la inacción con respecto a una reclamación presentada ante la autoridad u organismo mencionado en el artículo 63, apartado 1.

2. Los recursos presentados en aplicación del presente artículo se dirimirán en los tribunales del Estado miembro donde se encuentre la autoridad u organismo ante el cual se plantea el procedimiento judicial.

Artículo 65

Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables a los incumplimientos del presente título y de los esquemas 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 sin demora dicho régimen y dichas medidas, así como cualquier modificación posterior que les afecte.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 66

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 67

Evaluación y revisión

1. A más tardar el 28 de junio de 2024, y posteriormente cada cinco años, la Comisión evaluará el impacto, la eficacia y la eficiencia de ENISA 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 ENISA en respuesta a sus actividades. Si la Comisión considerara que el funcionamiento continuado de ENISA ha dejado de estar justificada con respecto a los objetivos, mandato y tareas que le fueron atribuidos, la Comisión podrá proponer que se modifique el presente Reglamento en lo que se refiere a las disposiciones relacionadas con ENISA.

2. La evaluación valorará también el impacto, la eficacia y la eficiencia de las disposiciones del título III del presente Reglamento en relación con los objetivos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión y de mejorar el funcionamiento del mercado interior.

3. La evaluación valorará si son necesarios requisitos esenciales de ciberseguridad para el acceso al mercado interior a fin de evitar que se introduzcan en el mercado de la Unión productos, servicios y procesos de TIC que no cumplan los requisitos de base en materia de ciberseguridad.

4. A más tardar el 28 de junio de 2024, y posteriormente cada cinco años, 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 68

Derogación y sucesión

1. Queda derogado el Reglamento (UE) n.º 526/2013, con efecto a partir del 27 de junio de 2019.

2. Las referencias al Reglamento (UE) n.º 526/2013 y a ENISA tal y como se establece por dicho Reglamento se entenderán hechas al presente Reglamento y a ENISA tal y como se establece por el presente Reglamento.

3. ENISA tal y como se establece por el presente Reglamento sucederá a la ENISA establecida por el Reglamento (UE) 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 del Consejo de Administración y del Comité Ejecutivo adoptadas de conformidad con el Reglamento (UE) n. °526/2013 seguirán siendo válidas, a condición de que cumplen con lo dispuesto en el presente Reglamento.

4. ENISA se establecerá por un período indefinido a partir del 27 de junio de 2019.

5. El director ejecutivo nombrado de conformidad con el artículo 24, apartado 4, del Reglamento (UE) n.º 526/2013 permanecerá en el cargo y ejercerá las funciones del director ejecutivo a que se refiere el artículo 20 del presente Reglamento para el resto del mandato del director ejecutivo. Las demás condiciones de su contrato se mantendrán inalteradas

6. Los miembros del Consejo de Administración y sus suplentes designados de conformidad con el artículo 6 del Reglamento (UE) n.º 526/2013 permanecerán en el cargo y ejercerán las funciones del Consejo de Administración a que se refiere el artículo 15 del presente Reglamento para el resto de su mandato.

Artículo 69

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*.

2. Los artículos 58, 60, 61, 63, 64 y 65, se aplicarán a partir del 28 de junio de 2021.

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

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

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, servicios o procesos 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, servicios o procesos 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, servicio o proceso de TIC que debe evaluarse, o el representante autorizado de ninguno de ellos. Dicha prohibición no será óbice para que se utilicen los productos de TIC evaluados necesarios para las actividades del organismo de evaluación de la conformidad o para que se utilicen dichos productos de TIC para fines personales.

5. Los organismos 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, servicios o procesos de TIC evaluados, ni representarán a las partes que participan en estas actividades. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad 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. Dicha prohibición se aplicará, en particular, a los servicios de consultoría.

6. Si un organismo de evaluación de la conformidad pertenece a una entidad o institución pública o es gestionado por esta, se garantizará y documentará la independencia y la inexistencia de conflictos de interés entre la autoridad nacional de certificación de la seguridad y el organismo de evaluación de la conformidad.

7. 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.

8. 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 que pueda influir en su apreciación o en los resultados de sus actividades de evaluación de la conformidad, incluidas las presiones o incentivos de índole financiera, en particular por lo que respecta a personas o grupos de personas que tengan algún interés en los resultados de esas actividades.

9. 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, con independencia de si dichas tareas las efectúa el propio organismo o si se realizan en su nombre y bajo su responsabilidad. Cualquier subcontratación o consulta de personal externo se documentará debidamente, no supondrá la participación de intermediarios y será objeto de un acuerdo escrito que regulará, entre otros aspectos, la confidencialidad y el conflicto de intereses. El organismo de evaluación de la conformidad en cuestión asumirá toda la responsabilidad de las tareas desempeñadas.

10. En todo momento, respecto a cada procedimiento de evaluación de la conformidad y cada tipo, categoría o subcategoría de productos, servicios o procesos 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 en virtud del artículo 61 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, servicio o proceso de TIC de que se trate y si el proceso de producción es en serie.

11. 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.

12. 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 de la conformidad 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.

13. Se garantizará la imparcialidad del organismo de evaluación de la conformidad, de sus máximos directivos, de las personas responsables de efectuar las actividades de evaluación de la conformidad, y de cualquier subcontratista.

14. La remuneración de los máximos directivos y de las personas responsables de efectuar las actividades de evaluación de la conformidad no dependerá del número de evaluaciones de la conformidad que efectúe ni de los resultados de dichas evaluaciones.

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

16. El organismo de evaluación de la conformidad y su personal, comités, filiales, subcontratistas y cualquier otra entidad o trabajador de organismos externos con los que esté asociado deberán mantener la confidencialidad y observar el secreto profesional acerca de toda la información obtenida en el marco de las tareas de evaluación de la conformidad realizadas en virtud del presente Reglamento o de cualquier disposición de Derecho nacional por la que se aplique, salvo cuando el Derecho de la Unión o de un Estado miembro al que están sometidas dichas personas requiera su divulgación con respecto a las autoridades competentes de los Estados miembros en que realice sus actividades. Se protegerán los derechos de propiedad intelectual. El organismo de evaluación de la conformidad contará con procedimientos documentados por lo que respecta a los requisitos establecidos en el presente punto.

17. Salvo en los casos especificados en el punto 16, los requisitos del presente anexo no impedirán en modo alguno los intercambios de información técnica y de orientaciones normativas entre un organismo de evaluación de la conformidad y una persona que solicite o esté valorando la posibilidad de solicitar la certificación.

18. Los organismos de evaluación de la conformidad funcionarán con arreglo a un conjunto de condiciones coherentes, justas y razonables que tengan en cuenta los intereses de las pequeñas y medianas empresas en relación con las tasas.

19. Los organismos de evaluación de la conformidad cumplirán los requisitos de la norma pertinente armonizada por el Reglamento (CE) n.º 765/2008 para la acreditación de los organismos de evaluación de la conformidad que certifiquen productos, servicios o procesos de TIC.

20. 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) n.º 765/2008 para la acreditación de los laboratorios que realicen ensayos.