Este texto es exclusivamente un instrumento de documentación y no surte efecto jurídico. Las instituciones de la UE no asumen responsabilidad alguna por su contenido. Las versiones auténticas de los actos pertinentes, incluidos sus preámbulos, son las publicadas en el Diario Oficial de la Unión Europea, que pueden consultarse a través de EUR-Lex. Los textos oficiales son accesibles directamente mediante los enlaces integrados en este documento

►B 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)

(DO L 151 de 7.6.2019, p. 15)

Modificado por:

		Diario Oficial		
		nº	página	fecha
►M1	Reglamento (UE) 2025/37 del Parlamento Europeo y del Consejo de 19 de diciembre de 2024	L 37	1	15.1.2025

▼B

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)

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

▼M1

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 y los servicios de seguridad gestionados en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

▼B

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;

▼B

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;

▼M1

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 productos, servicios o procesos de TIC o servicios de seguridad gestionados 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 o los servicios de seguridad gestionados incluidos en el ámbito de aplicación del esquema específico;

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

▼B

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;

▼M1

14 *bis*) «servicio de seguridad gestionado»: servicio prestado a un tercero que consiste en llevar a cabo o prestar asistencia para actividades relacionadas con la gestión de riesgos de ciberseguridad, como, por ejemplo, la gestión de incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría relacionada con la asistencia técnica, incluidos los conocimientos específicos;

▼B

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;

▼M1

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

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

22) «autoevaluación de la conformidad»: acción realizada por un fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados para evaluar si estos cumplen los requisitos de un esquema europeo de certificación de la ciberseguridad específico.

▼B

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.

▼B

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.

▼M1

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 europeo de certificación de la ciberseguridad de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados y reforzar así la confianza en el mercado interior digital y su competitividad.

▼B

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.

▼B

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 ([1]);

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.

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;

([1]) 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).

▼B

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.

▼B

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

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

▼M1

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 y servicios de seguridad gestionados, según lo establecido en el título III del presente Reglamento, por los siguientes medios:

▼B

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;

▼M1

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

▼B

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.

▼M1

3. ENISA recopilará y publicará directrices y formulará buenas prácticas en relación con los requisitos de ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados, en cooperación con las autoridades nacionales de certificación de la ciberseguridad y con el sector, de una manera formal, estructurada y transparente.

▼B

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.

▼M1

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 y los servicios de seguridad gestionados.

▼B

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

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;

▼B

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.

▼B

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;

▼B

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 ([1]) 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.

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.

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

▼B

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.

▼B

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.

▼B

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;

▼B

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.

▼B

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.

▼B

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.

▼B

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 [1] 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.

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.

[1] 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).

▼B

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.

▼B

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 ([1]) y 2015/444 ([2]) 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.

([1]) 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).

([2]) 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).

▼B

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.

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.

▼B

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 ([1]), 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.

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.

([1]) 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).

▼B

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 ([1]), 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) ([2]), 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 ([3]) 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.

([1]) 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).

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

([3]) 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).

▼B

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.

▼B

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.

▼B

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 ([1]). 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.

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.

([1]) 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).

▼B

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.

▼B

TÍTULO III

MARCO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD

▼M1

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 en el seno de la Unión y haciendo posible que, a escala de la Unión, se adopte un planteamiento armonizado 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 y los servicios de seguridad gestionados.

2. El marco europeo de certificación de la ciberseguridad definirá 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 tratados o las funciones o servicios que ofrecen, o a los que permitan acceder, dichos productos, servicios y procesos durante todo su ciclo de vida. Además, confirmará que los servicios de seguridad gestionados que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad y confidencialidad de los datos consultados, tratados, almacenados o transmitidos en relación con la prestación de tales servicios, y que tales servicios son prestados en todo momento con la competencia, pericia y experiencia necesarias por personal que posee un nivel suficiente y adecuado de los conocimientos técnicos pertinentes y de integridad profesional.

▼B

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.

▼M1

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

3. La inclusión de productos, servicios y procesos de TIC específicos, o de servicios de seguridad gestionados, o de categorías de estos, en el programa de trabajo evolutivo de la Unión se justificará sobre la base de uno o más de los siguientes motivos:

▼M1

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

▼B

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

c) la demanda del mercado;

▼M1

c *bis*) los avances tecnológicos y la disponibilidad y el desarrollo de esquemas de certificación de la ciberseguridad internacionales y normas internacionales y normas empleadas por la industria;

▼B

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

▼M1

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

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

▼M1

3. A la hora de preparar las propuestas de esquema, ENISA consultará a todas las partes interesadas de manera oportuna mediante un proceso de consulta formal, abierto, transparente e inclusivo. Al transmitir la propuesta de esquema a la Comisión con arreglo al apartado 6, ENISA facilitará información sobre la forma en que ha cumplido lo dispuesto en el presente apartado.

4. Para cada propuesta de esquema, ENISA creará un grupo de trabajo *ad hoc* con arreglo al artículo 20, apartado 4, con el objetivo de facilitar a ENISA asesoramiento y conocimientos específicos. Dichos grupos de trabajo incluirán, según proceda y sin perjuicio de los procedimientos y la discrecionalidad establecidos en el artículo 20, apartado 4, expertos de las administraciones públicas de los Estados miembros, de las instituciones, órganos y organismos de la Unión y del sector privado.

▼B

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.

▼M1

7. La Comisión, sobre la base de la propuesta de esquema preparada por ENISA, podrá adoptar actos de ejecución que establezcan esquemas de certificación de la ciberseguridad europeos para productos, servicios y procesos de TIC y servicios de seguridad gestionados que cumplan los requisitos pertinentes de los artículos 51, 51 *bis*, 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.

▼B

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.

▼M1

Artículo 49 bis

Información y consulta sobre los esquemas europeos de certificación de la ciberseguridad

1. La Comisión hará pública la información sobre su solicitud a ENISA para que esta prepare una propuesta de esquema o revise un esquema europeo de certificación de la ciberseguridad existente a que se refiere el artículo 48.

▼M1

2. Durante la preparación de una propuesta de esquema por parte de ENISA en virtud del artículo 49, el Parlamento Europeo, el Consejo o ambos, podrán solicitar a la Comisión, en su calidad de presidenta del GECC, y a ENISA, que presente trimestralmente información pertinente sobre una propuesta de esquema. A petición del Parlamento Europeo o del Consejo, ENISA, de acuerdo con la Comisión, y sin perjuicio de lo dispuesto en el artículo 27, podrá poner a disposición del Parlamento Europeo y del Consejo las partes pertinentes de una propuesta de esquema de un modo que se ajuste al nivel de confidencialidad requerido y, en su caso, de forma restringida.

3. Con el fin de reforzar el diálogo entre las instituciones de la Unión y contribuir a un proceso de consulta formal, abierto, transparente e inclusivo, el Parlamento Europeo, el Consejo o ambos, podrán invitar a la Comisión y a ENISA a debatir cuestiones relativas al funcionamiento de los esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC o servicios de seguridad gestionados.

4. La Comisión tendrá en cuenta, en su caso, los elementos derivados de las opiniones expresadas por el Parlamento Europeo y el Consejo, o por uno de ellos, sobre las cuestiones a que se refiere el apartado 3 del presente artículo al evaluar el presente Reglamento en virtud del artículo 67.

▼B

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

▼M1

Objetivos de seguridad de los esquemas europeos de certificación de la ciberseguridad en relación con los productos, servicios y procesos de TIC

Los esquemas europeos de certificación de la ciberseguridad en relación con los productos, servicios o procesos de TIC deberán diseñarse para cumplir, según proceda, al menos los objetivos de seguridad siguientes:

▼B

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.

▼M1

Artículo 51 bis

Objetivos de seguridad de los esquemas europeos de certificación de la ciberseguridad en relación con los servicios de seguridad gestionados

Los esquemas europeos de *certificación* de la ciberseguridad en relación con los servicios de seguridad gestionados deberán diseñarse para cumplir, según proceda, al menos los objetivos de seguridad siguientes:

a) que los servicios de seguridad gestionados se presten con la competencia, pericia y experiencia necesarias, y, en particular, que el personal encargado de prestar dichos servicios posea un nivel suficiente y adecuado de competencia y conocimientos técnicos en el ámbito específico, así como una experiencia suficiente y adecuada, y actúe con el máximo nivel de integridad profesional;

▼M1

b) que el proveedor disponga de procedimientos internos adecuados para asegurar que los servicios de seguridad gestionados se presten en todo momento con un nivel de calidad suficiente y adecuado;

c) que se protejan los datos consultados, almacenados, transmitidos o tratados de otro modo en relación con la prestación de servicios de seguridad gestionados frente al acceso, almacenamiento, revelación, destrucción u otro tipo de tratamiento accidentales o no autorizados, la pérdida o la alteración, o la falta de disponibilidad;

d) que se restauren la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico;

e) que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso;

f) que se lleve un registro y esté disponible para evaluar los datos, servicios o funciones que han sido objeto de acceso, uso u otro tratamiento, en qué momentos y por quién;

g) que los productos, servicios y procesos de TIC que se implementen en el contexto de la prestación de los servicios de seguridad gestionados sean seguros desde el diseño y por defecto, y, cuando proceda, incluyan las últimas actualizaciones de seguridad y no contengan vulnerabilidades conocidas públicamente.

▼B

Artículo 52

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

▼M1

1. Los esquemas europeos de certificación de la ciberseguridad podrán especificar uno o más de los niveles de garantía siguientes para los productos, servicios y procesos de TIC y los servicios de seguridad gestionados: «básico», «sustancial» o «elevado». El nivel de garantía deberá reflejar el nivel del riesgo asociado al uso previsto del producto, servicio o proceso de TIC o servicio de seguridad gestionado, en términos de probabilidad y repercusiones de un incidente.

▼B

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.

▼M1

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

▼B

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.

▼M1

5. Un certificado europeo de ciberseguridad o una declaración de conformidad de la UE que se refiere a un nivel de garantía «básico» ofrece garantías de que los productos, servicios y procesos de TIC o los servicios de seguridad gestionados para los cuales se expide 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 incidentes y ciberataques. Las actividades de evaluación que deberán 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 o los servicios de seguridad gestionados para los cuales se expide dicho certificado cumplen los requisitos de seguridad correspondientes, 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 que deberán efectuarse incluirán al menos: la revisión para demostrar la ausencia de vulnerabilidades conocidas públicamente y la comprobación de que los productos, servicios o procesos de TIC o los servicios de seguridad gestionados 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» ofrecerá garantías de que los productos, servicios y procesos de TIC o los servicios de seguridad gestionados para los cuales se expide dicho certificado cumplen los requisitos de seguridad correspondientes, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta nivel que pretende minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables. Las actividades de evaluación que deberán efectuarse incluirán al menos: la revisión para demostrar la improcedencia de las vulnerabilidades conocidas públicamente, la comprobación de que los productos, procesos o servicios de TIC o los servicios de seguridad gestionados aplican correctamente la funcionalidad de seguridad más con las tecnologías de vanguardia necesarias, y la evaluación de su resistencia a atacantes expertos mediante pruebas de penetración. Cuando dichas actividades de evaluación no sean apropiadas, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

▼B

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

▼M1

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 o servicios de seguridad gestionados. La autoevaluación de la conformidad únicamente se autorizará en relación con los productos, servicios y procesos de TIC o los servicios de seguridad gestionados que presenten un riesgo bajo correspondientes al nivel de garantía «básico».

2. El fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados puede expedir una declaración de conformidad de la UE en la que se indique que ha quedado demostrado el cumplimiento de los requisitos establecidos en el esquema. Al expedir dicha declaración, el fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados asumirá la responsabilidad de la conformidad del producto, servicio o proceso de TIC o servicio de seguridad gestionado con los requisitos que establezca dicho esquema.

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

▼B

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:

▼M1

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

▼B

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;

▼M1

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 aplicables a que se refieren los artículos 51 y 51 *bis*;

▼B

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;

▼M1

j) las normas para controlar el cumplimiento de los productos, servicios y procesos de TIC o los servicios de seguridad gestionados 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;

▼B

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;

▼M1

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

▼B

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

▼B

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

▼M1

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

▼B

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;

▼M1

q) el período de disponibilidad de la declaración de conformidad de la UE, la documentación técnica y cualquier otra información pertinente que deba facilitar el fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados;

▼B

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.

▼B

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

▼M1

1. Los productos, servicios y procesos de TIC y los servicios de seguridad gestionados que hayan sido certificados en virtud de un esquema europeo de certificación de la ciberseguridad adoptado con arreglo al artículo 49 se considerarán conformes con los requisitos de dicho esquema.

▼B

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. ►M1 La Comisión evaluará periódicamente la eficacia y la utilización de los esquemas europeos de certificación de la ciberseguridad adoptados, así como si un determinado esquema europeo de certificación de la ciberseguridad 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 y, a partir del 4 de febrero de 2025, los servicios de seguridad gestionados en la Unión y mejorar el funcionamiento del mercado interior. La primera de tales evaluaciones se efectuará a más tardar el 31 de diciembre de 2023, y las evaluaciones posteriores, como mínimo cada dos años. La Comisión deberá, a partir de los resultados de las evaluaciones, determinar los productos, servicios y procesos de TIC y los servicios de seguridad gestionados cubiertos por un esquema de certificación existente que deban estar cubiertos por un esquema de certificación obligatorio. ◄

▼B

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:

▼M1

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

▼B

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;

▼M1

d) tener en cuenta los plazos de aplicación, así como 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 o servicios de seguridad gestionados, incluidos los intereses y necesidades específicos de las pymes, incluidas las microempresas;

▼B

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.

▼B

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.

▼M1

7. La persona física o jurídica que presenta los productos, servicios o procesos de TIC o servicios de seguridad gestionados para la certificación pondrá a disposición de la autoridad nacional de certificación de la ciberseguridad designada en virtud del 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 de los productos, servicios o procesos de TIC o los servicios de seguridad gestionados certificados que pueda afectar al cumplimiento de los requisitos de certificación. Dicha autoridad u organismo transmitirá la información sin demora indebida a la autoridad nacional de certificación de la ciberseguridad de que se trate.

▼B

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

▼M1

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

▼M1

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

▼B

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.

▼B

7. Las autoridades nacionales de certificación de la ciberseguridad:

▼M1

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 y los servicios de seguridad gestionados con los requisitos de los certificados europeos de ciberseguridad que hayan sido expedidos en sus respectivos territorios, en cooperación con otras autoridades de vigilancia del mercado pertinentes;

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

▼B

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;

▼M1

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

▼B

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.

▼M1

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 y los servicios de seguridad gestionados.

▼B

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.

▼B

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;

▼M1

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

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

▼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.

▼B

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.

▼B

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;

▼B

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.

▼B

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.

▼M1

2. En la evaluación se analizarán también los efectos, la eficacia y la eficiencia de las disposiciones del título III del presente Reglamento, incluidos los procedimientos que conducen a la adopción de esquemas europeos de certificación de la ciberseguridad y sus bases empíricas, en relación con los objetivos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados en la Unión y de mejorar el funcionamiento del mercado interior.

3. En la evaluación se analizará la necesidad de establecer requisitos esenciales de ciberseguridad para el acceso al mercado interior a fin de evitar que se introduzcan en el mercado interior productos, servicios y procesos de TIC o servicios de seguridad gestionados que no sean conformes con los requisitos básicos en materia de ciberseguridad.

▼B

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.

▼B

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.

▼M1

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 o de los servicios de seguridad gestionados que evalúa.

3. Podrá tratarse de un organismo pertenecientes 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 o los servicios de seguridad gestionados 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 o del servicio de seguridad gestionado 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. El organismo de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, la fabricación o construcción, la prestación, la comercialización, la instalación, el uso o el mantenimiento de los productos, servicios o procesos de TIC o de los servicios de seguridad gestionados que son evaluados, ni representarán a las partes que participan en estas actividades. Los organismos de evaluación de la conformidad, sus máximos directivos y las personas responsables 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.

▼B

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.

▼B

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.

▼M1

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 o de servicios de seguridad gestionados, el organismo de evaluación de la conformidad dispondrá de:

▼B

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;

▼M1

c) 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 o servicio de seguridad gestionado de que se trate y si el proceso de producción es en serie.

▼B

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.

▼B

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.

▼M1

19. Los organismos de evaluación de la conformidad cumplirán los requisitos de la norma armonizada pertinente tal como se define en el artículo 2, punto 9, del 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 o servicios de seguridad gestionados.

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 armonizada pertinente tal como se define en el artículo 2, punto 9, del Reglamento (CE) n.º 765/2008 para la acreditación de los laboratorios que realicen ensayos.