17.4.2024 A9-0307/ 001-001

ENMIENDAS 001-001
presentadas por la Comisión de Industria, Investigación y Energía

Informe
Josianne Cutajar **A9-0307/2023**
Servicios de seguridad gestionados

Propuesta de Reglamento (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Enmienda 1

ENMIENDAS DEL PARLAMENTO EUROPEO*

a la propuesta de la Comisión

2023/0108 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados

(Texto pertinente a efectos del EEE)

* Enmiendas: el texto nuevo o modificado se señala en negrita y cursiva; las supresiones se indican mediante el símbolo ▌.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

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

Visto el dictamen del Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario[2],

---

1 ***DO C 349, de 29.9.2023, p. 167.***

2 ***Posición del Parlamento Europeo de ... (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de ….***

Considerando lo siguiente:

(1) El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[1] establece 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 de las tecnologías de la información y la comunicación*** (TIC), los servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

(1 bis) A fin de garantizar la resiliencia de la Unión frente a los ciberataques y prevenir cualquier vulnerabilidad en el mercado de la Unión, el presente Reglamento complementará el marco regulador horizontal que establece requisitos globales de ciberseguridad para todos los productos con elementos digitales de conformidad con el Reglamento (UE).../... del Parlamento Europeo y del Consejo [2] (2022/0272(COD)), estableciendo requisitos esenciales para los servicios gestionados en materia de ciberseguridad, su aplicación y su fiabilidad.

(2) Los servicios de seguridad gestionados, que consisten en llevar a cabo o prestar asistencia para actividades relacionadas con la gestión de los riesgos de ciberseguridad de los clientes de tales servicios, ***en particular la detección, la respuesta o la recuperación en caso de incidentes***, han ido adquiriendo cada vez más importancia en el contexto de la prevención y mitigación de incidentes de ciberseguridad. ***Las actividades de los proveedores de servicios de seguridad gestionados consisten en servicios relacionados con la prevención, la identificación, la protección, la detección, el análisis, la contención, la respuesta y la recuperación, incluidos, entre otros, la prestación de inteligencia sobre ciberamenazas, el seguimiento de amenazas en tiempo real mediante técnicas proactivas, incluida la seguridad desde el diseño, la evaluación de riesgos, la detección ampliada, la reparación y la respuesta.*** En consecuencia, los proveedores

---

1 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») (DO L 151 de 7.6.2019, p. 15).

2 Reglamento (UE) ... /... del Parlamento Europeo y del Consejo, de... sobre... (DOL, …, ELI: …).

de servicios de seguridad gestionados se consideran, de conformidad con la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[1], entidades esenciales o importantes pertenecientes a un sector de alta criticidad. De acuerdo con el considerando 86 de la citada Directiva, los proveedores de servicios de seguridad gestionados en ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría desempeñan un papel especialmente importante prestando asistencia a las entidades en sus esfuerzos de prevención, detección, respuesta y recuperación en relación con los incidentes. No obstante, los propios proveedores de servicios de seguridad gestionados también han sido víctimas de ciberataques y plantean un riesgo especial como consecuencia de su estrecha integración en las actividades de sus clientes. Por lo tanto, las entidades que se consideren esenciales e importantes de acuerdo con la Directiva (UE) 2022/2555 deben redoblar su diligencia a la hora de seleccionar un proveedor de servicios de seguridad gestionados.

(3) Los proveedores de servicios de seguridad gestionados también desempeñan un papel importante en el marco de la Reserva de Ciberseguridad de la UE, cuya creación gradual está respaldada por el Reglamento (UE) .../... [por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos]. Dicha Reserva de Ciberseguridad de la UE está destinada a utilizarse para prestar apoyo a acciones de respuesta y recuperación inmediata en caso de incidentes de ciberseguridad significativos y a gran escala. El Reglamento (UE) .../... [por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos] dispone un proceso para la selección de los proveedores que integren la Reserva de Ciberseguridad de la UE en el que, entre otros aspectos, debe tenerse en cuenta si el proveedor de que se trate ha obtenido una certificación de ciberseguridad a nivel nacional o europeo. Los servicios pertinentes prestados por «proveedores de confianza» de conformidad con el Reglamento

[1] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

(UE).../... [por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos] corresponden a los «servicios de seguridad gestionados» de conformidad con el presente Reglamento.

(4) La certificación de los servicios de seguridad gestionados no solo es pertinente en el marco del proceso de selección de la Reserva de Ciberseguridad de la UE, sino que constituye también un indicador de calidad fundamental para las entidades públicas y privadas que tengan intención de contratar esos servicios. En vista de la criticidad de los servicios de seguridad gestionados y de la sensibilidad de los datos tratados en relación con tales servicios, la certificación podría proporcionar importantes orientaciones y garantías sobre la fiabilidad de los servicios a los clientes potenciales. Los esquemas europeos de certificación en relación con los servicios de seguridad gestionados contribuyen a evitar la fragmentación del mercado único. Por consiguiente, el presente Reglamento tiene por objeto mejorar el funcionamiento del mercado interior.

(4 bis) Los esquemas europeos de certificación en relación con los servicios de seguridad gestionados deben conducir a la aceptación de dichos servicios y a una mayor competencia sobre el terreno, teniendo en cuenta las necesidades específicas tanto de los proveedores como de los beneficiarios. Esos esquemas deben, por tanto, lograr un equilibrio entre su objetivo y la posible carga normativa, administrativa y financiera que podrían afrontar los proveedores, especialmente las microempresas o las pequeñas y medianas empresas (pymes). Además, los esquemas deben fomentar el uso de servicios de seguridad gestionados certificados contribuyendo a su accesibilidad, especialmente para los agentes más pequeños, como las microempresas y las pymes, así como para las autoridades locales y regionales que tienen capacidades y recursos limitados, pero que son más propensos a vulnerar la ciberseguridad con implicaciones financieras, jurídicas, de reputación y operativas.

(4 ter) El esquema europeo de certificación en relación con los servicios de seguridad gestionados debe asegurar la disponibilidad de servicios seguros y de alta calidad que garanticen una transición digital segura y contribuyan a la consecución de los objetivos establecidos en el programa estratégico de la Década Digital,

especialmente en lo que se refiere a los objetivos de que el 75 % de las empresas de la Unión empiecen a utilizar computación en nube, inteligencia artificial o macrodatos, de que más del 90 % de las pymes alcancen al menos un nivel básico de intensidad digital y de que los servicios públicos esenciales se ofrezcan en línea.

(4 quater) En el panorama digital y tecnológico actual, en rápida evolución, la oferta de recursos educativos y la formación formal difieren y los conocimientos pueden adquirirse de diversas maneras, tanto formales como universitarias o cursos y no formales, por ejemplo, mediante la formación en el puesto de trabajo o una larga experiencia laboral en el ámbito pertinente.

(5) Además de la implementación de productos, servicios o procesos de TIC, los servicios de seguridad gestionados a menudo ofrecen características adicionales que dependen de las competencias, conocimientos especializados y experiencia del personal encargado de su prestación. A fin de garantizar que los servicios de seguridad gestionados que se presten sean de óptima calidad, debe exigirse, dentro de los objetivos de seguridad, un nivel muy elevado de dichas competencias, conocimientos especializados y experiencia, así como unos procedimientos internos adecuados. Para asegurar que todos los aspectos de un servicio de seguridad gestionado puedan estar cubiertos por un esquema de certificación ***específico***, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. El ***desarrollo del esquema de certificación establecido en virtud del presente Reglamento también debe tener en cuenta los resultados y las recomendaciones de la evaluación y revisión previstas en el presente Reglamento.***

(5 bis) Con el fin de facilitar el crecimiento de un mercado fiable de la Unión, al tiempo que se crean asociaciones con terceros países afines, también a la luz de las disposiciones del Reglamento (UE).../... del Parlamento Europeo y del Consejo[1] (2023/0109(COD)) en lo que respecta al acceso a la Reserva de Ciberseguridad de la UE, el proceso de certificación establecido en el marco establecido por el presente Reglamento debe racionalizarse para garantizar el reconocimiento internacional y la armonización con las normas internacionales.

---

1 Reglamento (UE) ... /... del Parlamento Europeo y del Consejo, de... sobre... (DOL, …, ELI: …). …).

(5 ter) Con el fin de garantizar el desarrollo de un mercado fiable de la Unión para los servicios de seguridad gestionados, los proveedores y los Estados miembros deben colaborar y contribuir a la recopilación de datos sobre la situación y la evolución del mercado laboral de ciberseguridad.

(5 quater) Un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas se basa en el desarrollo de capacidades de los Estados miembros. No obstante, la Unión se enfrenta a una brecha de talento, caracterizada por una escasez de profesionales cualificados, y a un panorama de amenazas en rápida evolución, como se reconoce en la Comunicación de la Comisión, de 18 de abril de 2023, sobre la Academia de Cibercapacidades. Por consiguiente, a fin de facilitar la aparición de servicios de seguridad gestionados esenciales y de alta calidad y tener una mejor visión de conjunto de la composición de la mano de obra de la Unión en materia de ciberseguridad, debe reforzarse la cooperación entre los Estados miembros, la Comisión, la ENISA y las partes interesadas, incluidos el sector privado y el mundo académico, mediante el desarrollo de asociaciones público-privadas, el apoyo a iniciativas de investigación e innovación, el desarrollo y el reconocimiento mutuo de normas comunes y la certificación de capacidades en materia de ciberseguridad, también a través del Marco Europeo de Capacidades en Ciberseguridad. Todo ello debería facilitar la movilidad de los profesionales de la ciberseguridad dentro de la Unión, así como la integración de los conocimientos y la formación en materia de ciberseguridad en los programas educativos, garantizando al mismo tiempo el acceso a la formación de aprendices y a los períodos de prácticas para los jóvenes, especialmente las personas que viven en regiones desfavorecidas, como las islas y las zonas escasamente pobladas, rurales y remotas. Estas medidas también deben tener por objeto atraer a más mujeres y niñas en este ámbito y contribuir a abordar la brecha de género en la ciencia, la tecnología, la ingeniería y las matemáticas. El sector privado también debe aspirar a impartir formación en el puesto de trabajo que aborde las capacidades más demandadas, con la participación de la administración pública y las empresas emergentes, así como las microempresas y las pequeñas y medianas empresas.

(5 quinquies) Deben garantizarse la financiación y los recursos adecuados a efectos de las tareas adicionales encomendadas a ENISA mediante las modificaciones al Reglamento (UE) 2019/881 introducidas por el presente Reglamento.

(5 sexies) A fin de completar determinados elementos no esenciales del presente Reglamento, deben delegarse en la Comisión los poderes para adoptar actos, de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea para proporcionar un esquema europeo de certificación de la ciberseguridad para los productos, los servicios y procesos de TIC y los servicios de seguridad gestionados Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[1]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(5 septies) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, emitió su dictamen el [DD/MM/AAAA][2].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

---

1 DO L 123, de 12.5.2016, p. 1.

2 ***DO C .../…***

Artículo 1

Modificaciones del Reglamento (UE) 2019/881

El Reglamento (UE) 2019/881 se modifica como sigue:

1) En el artículo 1, apartado 1, párrafo primero, la letra b) se sustituye por el texto siguiente:

«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.».

2) El artículo 2 se modifica como sigue:

a) Los puntos 9, 10 y 11 se sustituyen por el texto siguiente:

«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 y 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) Se inserta el punto siguiente:

«14 bis) "servicio de seguridad gestionado": servicio ***prestado a un tercero*** que consiste en llevar a cabo o prestar asistencia, o ***asesoramiento*** para actividades relacionadas con la gestión de riesgos de ciberseguridad, en particular, ***la gestión de incidentes***, las pruebas de penetración, las auditorías de seguridad y la consultoría;».

c) Los puntos 20, 21 y 22 se sustituyen por el texto siguiente:

«20) "especificaciones técnicas": 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 los mismos;

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 específico de certificación de la ciberseguridad; 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 específico de certificación de la ciberseguridad.».

3) En el artículo 4, el apartado 6 se sustituye por el texto siguiente:

«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.».

4) El artículo 8 se modifica como sigue:

a) El apartado 1 se sustituye por el texto siguiente:

«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:

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

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

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

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

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

b) El apartado 3 se sustituye por el texto siguiente:

«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.».

c) El apartado 5 se sustituye por el texto siguiente:

«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.».

5) En el artículo 46, los apartados 1 y 2 se sustituyen por el texto siguiente:

«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 miras a 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 define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad. Este mecanismo confirma 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 ofrezcan, o a los que permitan acceder, dichos productos, servicios y procesos durante todo su ciclo de vida. Además, confirma 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 muy elevado de los conocimientos técnicos pertinentes y de integridad profesional.».

6) En el artículo 47, los apartados 2 y 3 se sustituyen por el texto siguiente:

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

ciberseguridad. ***En este contexto, la Comisión podrá incluir una evaluación en profundidad de las vías de formación existentes para colmar las carencias de capacidades detectadas y una lista de propuestas para abordar las necesidades de los trabajadores cualificados y los tipos de capacidades.***

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

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

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

c) la demanda del mercado;

c bis) los avances tecnológicos y la disponibilidad y el desarrollo de regímenes internacionales de certificación de la ciberseguridad y normas internacionales e industriales.

d) la evolución del panorama de las ciberamenazas;

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

7) El artículo 49 ***se modifica como sigue***:

a) El apartado 7 se sustituye por el texto siguiente:

«7. La Comisión, a partir de la propuesta de esquema preparada por ENISA, ***está facultada para adoptar actos delegados de conformidad con el artículo 65bis, que complementen el presente Reglamento mediante el establecimiento*** de esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC y servicios de seguridad gestionados que cumplan los requisitos de los artículos 51, 52

y 54.

b) se inserta el apartado siguiente:

«7 bis. Antes de adoptar dichos actos delegados, la Comisión, en cooperación con ENISA, llevará a cabo y publicará una evaluación de impacto del esquema europeo de certificación de la ciberseguridad propuesto. Al preparar la evaluación de impacto, la Comisión realizará consultas públicas y consultas con el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad y el Grupo Europeo de Certificación de la Ciberseguridad.

8) El artículo 51 se modifica como sigue:

a) El título se sustituye por el texto siguiente:

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

b) La parte introductoria se sustituye por el texto siguiente:

«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:»

9) Se inserta el artículo siguiente:

«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) garantizar 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 muy elevado 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;

b) garantizar 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 muy elevado;

c) proteger 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) garantizar 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) garantizar que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiera su derecho de acceso;

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

g) garantizar 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 por defecto y desde el diseño ***y se entreguen con un programa informático y un equipo informático actualizados***, no contengan vulnerabilidades conocidas e incluyan las últimas actualizaciones de seguridad.

10) El artículo 52 se modifica como sigue:

a) El apartado 1 se sustituye por el texto siguiente:

«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) El apartado 3 se sustituye por el texto siguiente:

«3. Los requisitos de seguridad relativos a cada nivel de garantía se precisarán en el esquema europeo de certificación de la ciberseguridad pertinente, con inclusión de las correspondientes funcionalidades de seguridad y el correspondiente rigor y exhaustividad de la evaluación a la que debe someterse el producto, servicio o proceso de TIC o el servicio de seguridad gestionado.».

c) Los apartados 5, 6 y 7 se sustituyen por el texto siguiente:

«5. El certificado europeo de ciberseguridad o la declaración de conformidad de la UE que se refiera a un nivel de garantía "básico" ofrecerá garantías de que los productos, servicios y procesos de TIC y los servicios de seguridad gestionados para los cuales se expida cumplen los requisitos de seguridad correspondientes, incluidas las funcionalidades de seguridad, y se han evaluado a un nivel que pretende minimizar los riesgos básicos conocidos de incidentes y ciberataques. Las actividades de evaluación que deberán efectuarse comprenderán al menos el examen de la documentación técnica. Cuando dicho examen no sea adecuado, se recurrirá a actividades de evaluación alternativas con efecto equivalente.

6. El certificado europeo de ciberseguridad que se refiera a un nivel de garantía "sustancial" ofrecerá garantías de que los productos, servicios y procesos de TIC y los servicios de seguridad gestionados para los cuales se expida cumplen los requisitos de seguridad correspondientes, incluidas las funcionalidades de seguridad, y se han evaluado a un nivel que pretende minimizar los riesgos de ciberseguridad conocidos, así como el riesgo de incidentes y ciberataques cometidos por agentes con capacidades y recursos limitados. Las actividades de evaluación que deberán efectuarse comprenderán al menos lo siguiente: un examen para demostrar la ausencia de vulnerabilidades conocidas públicamente y pruebas para demostrar 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 adecuadas, se recurrirá a actividades de evaluación alternativas con efecto equivalente.

7. El certificado europeo de ciberseguridad que se refiera a un nivel de garantía "elevado" ofrecerá garantías de que los productos, servicios y procesos de TIC y los servicios de seguridad gestionados para los cuales se expida cumplen los requisitos de seguridad correspondientes, incluidas las funcionalidades de seguridad, y se han evaluado a un nivel que pretende minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables. Las actividades de evaluación que deberán efectuarse comprenderán al menos lo siguiente: un examen para demostrar la ausencia de vulnerabilidades conocidas públicamente, pruebas para demostrar que los productos, procesos o servicios de TIC o los servicios de seguridad gestionados aplican correctamente las funcionalidades de seguridad más avanzadas necesarias, y una evaluación, mediante pruebas de penetración, de la resistencia a atacantes expertos. Cuando dichas actividades de evaluación no sean adecuadas, se recurrirá a actividades de evaluación alternativas con efecto equivalente.».

11) En el artículo 53, los apartados 1, 2 y 3 se sustituyen por el texto siguiente:

«1. Los esquemas europeos de certificación de la ciberseguridad podrán permitir la 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 y los servicios de seguridad gestionados que presenten un riesgo bajo correspondiente al nivel de garantía "básico".

2. El fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados podrá emitir 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 emitir dicha declaración, el fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados asumirá la responsabilidad respecto de la conformidad del producto, servicio o proceso de TIC o servicio de seguridad gestionado con los requisitos del esquema pertinente.

3. El fabricante o proveedor de productos, servicios o procesos de TIC o servicios de seguridad gestionados pondrá a disposición de la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 58, durante el período previsto en el esquema europeo de certificación de la ciberseguridad correspondiente, la declaración de conformidad de la UE, la documentación técnica y cualquier otra información pertinente en relación con la conformidad de los productos, servicios o procesos de TIC o los servicios de seguridad gestionados con el esquema. Deberá presentarse una copia de la declaración de conformidad de la UE a la autoridad nacional de certificación de la ciberseguridad y a ENISA.».

12) En el artículo 54, el apartado 1 se modifica como sigue:

a) La letra a) se sustituye por el texto siguiente:

«a) el objeto y el alcance del esquema de certificación, incluido el tipo o las categorías de productos, servicios y procesos de TIC y servicios de seguridad gestionados cubiertos;».

b) La letra j) se sustituye por el texto siguiente:

«j) las normas 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 o las declaraciones de conformidad de la UE, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;».

c) La letra l) se sustituye por el texto siguiente:

«l) las normas relativas a las consecuencias para los productos, servicios y procesos de TIC y los servicios de seguridad gestionados que hayan 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;».

d) La letra o) se sustituye por el texto siguiente:

«o) las referencias a los esquemas nacionales o internacionales de

certificación de la ciberseguridad que cubran el mismo tipo o categoría de productos, servicios y procesos de TIC y servicios de seguridad gestionados, requisitos de seguridad, criterios y métodos de evaluación y niveles de garantía;».

e) La letra q) se sustituye por el texto siguiente:

«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;».

13) El artículo 56 se modifica como sigue:

a) El apartado 1 se sustituye por el texto siguiente:

«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) El apartado 3 se modifica como sigue:

i) El párrafo primero se sustituye por el texto siguiente:

«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 pertinente para garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC y 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.».

ii) El párrafo tercero se modifica como sigue:

a bis) La letra a) se sustituye por el texto siguiente:

«a) tener en cuenta las repercusiones de las medidas, en términos de costes, sobre los fabricantes o proveedores de dichos productos, servicios o procesos de TIC o servicios de seguridad gestionados y sobre los usuarios, 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 ter) La letra d) se sustituye por el texto siguiente:

«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 proveedores de productos, servicios o procesos de TIC o servicios de seguridad gestionados, incluidos ***los intereses específicos y las necesidades de las microempresas y las pymes***;»;

iii) se añade el párrafo siguiente:

«Con respecto al párrafo tercero, letra d), del presente artículo, la Comisión garantizará un apoyo financiero adecuado en el marco regulador de los programas de la Unión existentes, en particular para aliviar la carga financiera de las microempresas y las pymes, incluidas las empresas emergentes que actúan en el ámbito de los servicios de seguridad gestionados.».

c) Los apartados 7 y 8 se sustituyen por el texto siguiente:

«7. La persona física o jurídica que someta a certificación productos, servicios o procesos de TIC o servicios de seguridad gestionados pondrá a disposición de la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 58, si dicha autoridad es el organismo que expide el certificado europeo de ciberseguridad, o del

organismo de evaluación de la conformidad a que se refiere el artículo 60, toda la información necesaria para llevar a cabo el procedimiento de certificación.

8. El titular de un certificado europeo de ciberseguridad informará a la autoridad o al organismo a que se refiere el apartado 7 de cualquier vulnerabilidad o irregularidad que se detecte posteriormente en relación con la seguridad de los productos, servicios o procesos de TIC o los servicios de seguridad gestionados certificados que pueda afectar a su conformidad con los requisitos de certificación. Dicha autoridad u organismo transmitirá la información sin demora indebida a la autoridad nacional de certificación de la ciberseguridad correspondiente.».

14) En el artículo 57, los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Sin perjuicio de lo dispuesto en el apartado 3 del presente artículo, 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 estén cubiertos por un esquema europeo de certificación de la ciberseguridad dejarán de surtir efectos a partir de la fecha establecida en el ***acto delegado*** 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 en vigor.

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 que ya estén cubiertos por un esquema europeo de certificación de la ciberseguridad en vigor.».

15) El artículo 58 se modifica como sigue:

a) El apartado 7 se modifica como sigue:

i) Las letras a) y b) se sustituyen por el texto siguiente:

«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 lleven a cabo autoevaluaciones de la conformidad, y, en particular, controlarán el cumplimiento y velarán por la aplicación de las obligaciones que incumban a dichos fabricantes o proveedores en virtud del artículo 53, apartados 2 y 3, y del correspondiente esquema europeo de certificación de la ciberseguridad;».

ii) La letra h) se sustituye por el texto siguiente:

«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 y servicios de seguridad gestionados que pudieran no ser conformes con los requisitos del presente Reglamento o de esquemas europeos de certificación de la ciberseguridad específicos, y».

b) El apartado 9 se sustituye por el texto siguiente:

«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.».

16) En el artículo 59, apartado 3, las letras b) y c) se sustituyen por el texto siguiente:

«b) los procedimientos de supervisión y garantía del 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 garantía del 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);»;

16 bis) Se inserta el artículo siguiente:

«Artículo 65bis
Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 49, apartado 7, se otorgan a la Comisión por un período de cinco años a partir del ... [fecha de entrada en vigor del presente Reglamento modificado]. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 7 podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 49, apartado 7, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

17) El artículo 67 se sustituye por el texto siguiente:

«Artículo 67

Evaluación y revisión

1. A más tardar el 28 de junio de 2024, y posteriormente cada cuatro años, la Comisión valorará 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 justificado con respecto a los objetivos, mandato y tareas que le fueron atribuidos, la Comisión podrá proponer que se modifique el presente Reglamento en lo que se refiere a las disposiciones relacionadas con ENISA.

2. En la evaluación se analizarán las repercusiones, la eficacia y la eficiencia de las disposiciones del título III del presente Reglamento en relación con los objetivos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados en la Unión y de mejorar el funcionamiento del mercado interior.

3. La evaluación también valorará:

a) la eficiencia y la eficacia de los procedimientos conducentes a la consulta, preparación y adopción de regímenes europeos de certificación de la ciberseguridad, así como las formas de mejorar y acelerar dichos procedimientos;

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

4. A más tardar el 28 de junio de 2024, y posteriormente cada tres 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 2

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

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

Hecho en ...

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