Enmienda 2
Cristian-Silviu Buşoi
en nombre de la Comisión de Industria, Investigación y Energía

Informe **A9-0307/2023**
Josianne Cutajar
Servicios de seguridad gestionados
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Propuesta de Reglamento
–

ENMIENDAS DEL PARLAMENTO EUROPEO*

a la propuesta de la Comisión

REGLAMENTO (UE) 2024/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de …

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)

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,

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

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

Previa consulta al 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 … [(DO …) / (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[3] 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, servicios y procesos de ***las tecnologías de la información y la comunicación (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.

(2) 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[4] ***(2022/0272(COD)), estableciendo requisitos esenciales para los servicios gestionados en materia de ciberseguridad, su aplicación y su fiabilidad.***

---

3 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).

4 ***Reglamento (UE) …/… del Parlamento Europeo y del Consejo, de … sobre … (DO L, …, ELI: …).***

(3) Los servicios de seguridad gestionados ***son servicios prestados por proveedores de servicios de seguridad gestionados en el sentido del artículo 6, punto 40, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[5]. Por lo tanto, la definición de servicios de seguridad gestionados en el presente Reglamento debe ser coherente con la definición de proveedores de servicios de seguridad gestionados establecida en la Directiva (UE) 2022/2555. Estos servicios*** 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 ***y*** han ido adquiriendo cada vez más importancia en el contexto de la prevención y mitigación de incidentes de ciberseguridad. En consecuencia, los proveedores de servicios de seguridad gestionados se consideran, de conformidad con la Directiva (UE) 2022/2555 ▌, 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.

---

5 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).

(4) La definición de servicios de seguridad gestionados en el presente Reglamento incluye una lista no exhaustiva de servicios de seguridad gestionados que podrían acogerse a esquemas de certificación, como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría relacionada con la asistencia técnica. Los servicios de seguridad gestionados podrían abarcar servicios de ciberseguridad que ayudan en la preparación, la prevención, la detección, el análisis, la mitigación, la respuesta y la recuperación de incidentes de ciberseguridad. El suministro de información sobre ciberamenazas y la evaluación de riesgos relacionados con la asistencia técnica también podrían considerarse servicios de seguridad gestionados. Pueden existir diferentes esquemas europeos de certificación de la ciberseguridad para diferentes servicios de seguridad gestionados. Los certificados europeos de ciberseguridad expedidos de conformidad con dichos esquemas deben referirse a servicios de seguridad gestionados específicos de un proveedor específico de tales servicios.

(5) Los proveedores de servicios de seguridad gestionados también ***pueden desempeñar*** un papel importante en ***relación con las*** acciones de ***apoyo a la*** respuesta y recuperación inmediata ***de la Unión*** en caso de incidentes de ciberseguridad significativos y a gran escala***, basándose en servicios de proveedores de confianza y en la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en las evaluaciones de riesgos de la Unión. La certificación de los servicios de seguridad gestionados puede ser importante en la selección de los*** proveedores de confianza ▌ .

(6) 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.

(7) ***Los esquemas europeos de certificación en relación con los servicios de seguridad gestionados deben conducir a la adopción de dichos servicios y a una mayor competencia entre los proveedores de servicios de seguridad gestionados. Sin perjuicio del objetivo de garantizar unos niveles suficientes y adecuados de conocimientos técnicos pertinentes e integridad profesional de dichos proveedores, los esquemas de certificación deben, por tanto, facilitar la entrada en el mercado y la oferta de servicios de seguridad gestionados, simplificando, en la medida de lo posible, la potencial carga normativa, administrativa y financiera que podría recaer en los proveedores, especialmente las microempresas y las pequeñas y medianas empresas (pymes), al ofrecer servicios de seguridad gestionados. Además, con el fin de fomentar la adopción de servicios de seguridad gestionados y estimular la demanda de tales servicios, los esquemas deben contribuir 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.***

(8) ***Es importante ofrecer apoyo a las microempresas y a las pequeñas y medianas empresas (pymes) en la aplicación del presente Reglamento y en la obtención de las capacidades y conocimientos especializados de ciberseguridad necesarios para prestar servicios de seguridad gestionados conforme a los requisitos establecidos en el presente Reglamento. El programa Europa Digital y otros programas pertinentes de la Unión prevén que la Comisión debe establecer un apoyo financiero y técnico que permita a estas empresas contribuir al crecimiento de la economía europea y al fortalecimiento de un nivel común de ciberseguridad europea en el panorama de la Unión, en particular racionalizando el apoyo financiero del programa Europa Digital y otros programas pertinentes de la Unión y apoyando a las microempresas y las pymes.***

(9) ***El esquema de certificación de la Unión en relación con los servicios de seguridad gestionados debe contribuir a la disponibilidad de servicios seguros y de alta calidad que garanticen una transición digital segura y 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 microempresas y pymes alcancen al menos un nivel básico de intensidad digital y de que los servicios públicos esenciales se ofrezcan en línea.***

(10) 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 ***los servicios*** de seguridad ***gestionados*** puedan estar cubiertos por ***esquemas*** de certificación ***específicos***, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. ***Deben tenerse en cuenta los resultados y recomendaciones de la evaluación y revisión previstas en el*** Reglamento (UE) ***2019/881.***

(11) Con el fin de facilitar el crecimiento de un mercado fiable de la Unión, al tiempo que se crean asociaciones con terceros países afines, el proceso de certificación previsto en el marco establecido por el presente Reglamento debe racionalizarse para facilitar el reconocimiento internacional y la armonización con las normas internacionales.

(12) 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. Los recursos educativos y la oferta de formación formal difieren y los conocimientos pueden adquirirse de diversas maneras, tanto formales, por ejemplo, a través de la universidad u otros cursos, como no formales, por ejemplo, mediante la formación en el puesto de trabajo o la experiencia profesional en el ámbito pertinente. 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, es importante reforzar 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. Tal cooperación también facilitaría 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 de las personas jóvenes a períodos de prácticas y aprendizaje profesional, especialmente de las personas que viven en regiones desfavorecidas, como las islas y las zonas escasamente pobladas, rurales y remotas. Es importante que estas medidas tengan el objetivo de atraer a más mujeres y niñas a este ámbito y contribuyan a superar la brecha de género en la ciencia, la tecnología, la ingeniería y las matemáticas, y que el sector privado trate de 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 pymes. Asimismo, es importante que los proveedores y los Estados miembros colaboren y contribuyan a la recopilación de datos sobre la situación y la evolución del mercado laboral en el ámbito de la ciberseguridad.

(13) ENISA desempeña un papel importante en la preparación de las propuestas de esquemas europeos de certificación. Al preparar el proyecto de presupuesto general de la Unión, la Comisión debe evaluar los recursos presupuestarios necesarios para la plantilla de personal de ENISA, de conformidad con el procedimiento establecido en el artículo 29 del Reglamento (UE) 2019/881.

(14) El presente Reglamento prevé modificaciones específicas del Reglamento (UE) 2019/881 para añadir la posibilidad de crear esquemas de certificación de la ciberseguridad para los proveedores de servicios de seguridad gestionados. Al hacerlo, también especifica y aclara determinadas disposiciones relativas a la preparación y el funcionamiento de todos los esquemas europeos de certificación de la ciberseguridad con vistas a garantizar su transparencia y apertura. Estas últimas modificaciones, que se limitan a la especificación o aclaración del Reglamento (UE) 2019/881, en particular las modificaciones de los artículos 49 y 49 bis, no deben prejuzgar en modo alguno la evaluación y revisión más amplias de dicho Reglamento que exige su artículo 67, incluida específicamente la evaluación del impacto, la eficacia y la eficiencia del título de dicho Reglamento relativo al marco de certificación de la ciberseguridad. La evaluación y revisión del título relativo al marco de certificación de la ciberseguridad deben basarse en una consulta amplia a las partes interesadas y en un análisis completo y exhaustivo de los procedimientos pertinentes.

(15) ***Dado que el objetivo del presente Reglamento, a saber, facilitar la adopción de esquemas europeos de certificación de la ciberseguridad para los proveedores de servicios de seguridad gestionados, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a su dimensión y efectos, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.***

(16) ***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[6], emitió su dictamen el 10 de enero de 2024[7].***

HAN ADOPTADO EL PRESENTE REGLAMENTO:

---

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

7 ***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 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, incluido el asesoramiento de expertos;***»;

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 ***suficiente y adecuado*** 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.

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 esquemas 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) los apartados 1, 2, 3 y 4 se sustituyen por el texto siguiente:

«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.

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, de conformidad con el artículo 49, apartado 6, ENISA facilitará información sobre cómo ha cumplido esta obligación.

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. Los grupos de trabajo ad hoc creados a tal fin 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) el apartado 7 se sustituye por el texto siguiente:

«7. La Comisión, a partir de la propuesta de esquema preparada por ENISA, podrá adoptar actos de ejecución que establezcan esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC y servicios de seguridad gestionados que cumplan los requisitos 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.».

8) Se inserta el artículo siguiente:

«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.

2. Durante la preparación de una propuesta de esquema por parte de ENISA de conformidad con el artículo 49, el Parlamento Europeo y el Consejo podrán solicitar a la Comisión, en su calidad de presidenta del Grupo Europeo de Certificación de la Ciberseguridad (GECC) y de 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 y el Consejo 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 sobre las cuestiones a que se refiere el apartado 3 del presente artículo al evaluar el presente Reglamento de conformidad con el artículo 67.».

9) 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:».

10) 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) ▌ 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;

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 registre***, y ***se permita*** evaluar, qué datos, servicios o funciones 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 por defecto y desde el diseño***, y, cuando proceda***, incluyan las últimas actualizaciones de seguridad ***y no contengan vulnerabilidades conocidas públicamente***.».

11) 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.».

12) 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.».

13) 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;»;

a bis) la letra g) se sustituye por el texto siguiente:

«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) 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;».

14) 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:

aa) 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;»;

bb) 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 y necesidades específicos de las microempresas y*** las pymes;»;

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.».

15) 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 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 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.».

16) 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.».

17) 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);».

18) En el artículo 67, los apartados 2 y 3 se sustituyen por el texto siguiente:

«2. En la evaluación se analizarán también las repercusiones, la eficacia y la eficiencia de las disposiciones del título III del presente Reglamento***, incluidos los procedimientos que conducen a la adopción de esquemas 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 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.».

19) El anexo se sustituye por el texto que figura en el anexo del presente Reglamento.

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 ..., el ...

Por el Parlamento Europeo	*Por el Consejo*
[El Presidente / La Presidenta]	*[El Presidente / La Presidenta]*

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. ***Los organismos de evaluación de la conformidad se establecerán de conformidad con el Derecho interno y tendrán personalidad jurídica.***
2. ***Los organismos de evaluación de la conformidad serán organismos terceros independientes de la organización, de los productos, servicios o procesos de TIC o de los servicios de seguridad gestionados que evalúan.***
3. ***Podrá tratarse de organismos 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 evalúan, a condición de que se demuestre su independencia y la ausencia de conflictos de intereses.***
4. ***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 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. ***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 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.

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 intereses entre la autoridad nacional de certificación de la ciberseguridad y el organismo de evaluación de la conformidad.

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

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

9. Los organismos de evaluación de la conformidad deberán ser capaces de llevar a cabo todas las tareas de evaluación de la conformidad que les hayan sido asignadas en virtud del presente Reglamento, con independencia de si dichas tareas las efectúan los propios organismos 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 los conflictos de intereses. Los organismos de evaluación de la conformidad en cuestión asumirán toda la responsabilidad de las tareas desempeñadas.

10. En todo momento, respecto a cada procedimiento de evaluación de la conformidad y cada tipo, categoría o subcategoría de productos, servicios o procesos de TIC o de

servicios de seguridad gestionados, los organismos de evaluación de la conformidad dispondrán de:

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

b) 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. Dispondrán asimismo de las políticas y procedimientos adecuados que permitan distinguir entre las tareas efectuadas en tanto que organismos notificados en virtud del artículo 61 y cualquier otra actividad;

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.

11. Los organismos de evaluación de la conformidad dispondrán de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrán acceso a todos los equipos e instalaciones que necesiten.

12. Las personas que efectúen las actividades de evaluación de la conformidad tendrán:

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 efectúen 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 de la conformidad.

13. Se garantizará la imparcialidad de los organismos 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 efectúen ni de los resultados de dichas evaluaciones.

15. Los organismos de evaluación de la conformidad suscribirán 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. Los organismos de evaluación de la conformidad y su personal, comités, filiales, subcontratistas y cualquier otra entidad o trabajador de organismos externos con los que estén asociados 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. Los organismos de evaluación de la conformidad contarán con procedimientos documentados por lo que respecta a los requisitos establecidos en el presente punto.

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

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

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

Or. en