Parlamento Europeo
2019-2024

Comisión de Industria, Investigación y Energía

2023/0108(COD)

21.9.2023

ENMIENDAS
17 - 52

Proyecto de informe
Josianne Cutajar
(PE752.802v01-00)

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

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

Enmienda 17
Evžen Tošenovský

Propuesta de Reglamento
Considerando 2

Texto de la Comisión	*Enmienda*
(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, 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 ***del Parlamento Europeo y del Consejo***[8], 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.	(2) Los servicios de seguridad gestionados ***son servicios prestados por los proveedores de servicios de seguridad gestionados de conformidad con el artículo 6, punto 40, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo. Dichos servicios***, 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, 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 ***el anexo I, punto 10, de*** 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.

[8] 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).

[8] 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).

Or. en

Enmienda 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Considerando 2

Texto de la Comisión	*Enmienda*
(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, 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 del Parlamento Europeo y del Consejo[8], 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	(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 prevención, la detección, la respuesta y la recuperación en relación con los incidentes,*** 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 del Parlamento Europeo y del Consejo[8], 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

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.

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.

---

[8] 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).

[8] 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).

Or. en

Enmienda 19
Evžen Tošenovský

Propuesta de Reglamento
Considerando 3

Texto de la Comisión	*Enmienda*
(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	(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 (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***.	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 ***de servicios de seguridad gestionados de confianza*** 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. ***Además, cuando se disponga de un esquema europeo*** de ***certificación*** de ***la ciberseguridad en relación*** con ***los servicios de seguridad gestionados,*** que ***sustituiría también*** a ***todos los esquemas nacionales de certificación de*** la ***ciberseguridad pertinentes, debe aplicarse una certificación obligatoria*** de ***conformidad con dicho esquema de certificación que incluya*** a los ***proveedores de servicios*** de seguridad ***gestionados*** de ***confianza en la Reserva de Ciberseguridad de la UE***.
	Or. en

Enmienda 20
Johan Nissinen

Propuesta de Reglamento
Considerando 4

Texto de la Comisión	*Enmienda*
(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) 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. ***Al mismo tiempo, estos múltiples objetivos del Reglamento deben encontrar un equilibrio con la posible carga normativa y los costes asociados a la certificación, dado que el cumplimiento de los requisitos de certificación conllevará gastos y esfuerzos administrativos adicionales, lo que podría ser motivo de preocupación para los proveedores más pequeños.***

Or. en

Enmienda 21
Ville Niinistö
en nombre del Grupo Verts/ALE

Propuesta de Reglamento
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) Dado que el mercado y los sistemas educativos ofrecen una variedad de recursos educativos y formación formal, debe subrayarse que el conocimiento también se adquiere por vías no formales y que las capacidades pueden demostrarse, aunque no exclusivamente, a través de titulaciones y certificaciones. Especialmente en vista de la rápida evolución del panorama de amenazas actual, los Estados miembros y los beneficiarios de los servicios de seguridad gestionados deben tener en cuenta a los investigadores en materia de vulnerabilidades altamente cualificados. Además, dado que en algunos Estados miembros las personas físicas y entidades que investigan vulnerabilidades pueden incurrir en responsabilidad civil y penal, se alienta a los Estados miembros a que emitan directrices para que no se actúe penalmente cuando se trate de investigaciones en materia de seguridad de la información y formulen una excepción en cuanto a la responsabilidad civil por dichas actividades.

Or. en

Justificación

El panorama de los profesionales de la seguridad varía en parte debido a la diversidad de trayectorias profesionales no normalizadas, al acceso a la educación formal y a los recursos para obtener la certificación. Por lo tanto, debemos fomentar el empleo de personas cualificadas y garantizar un marco positivo para las actividades que conllevan una mejora de la ciberseguridad.

Enmienda 22
Josianne Cutajar

Propuesta de Reglamento
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) El esquema de certificación de la Unión 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[8 bis], 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.
	[8 bis] Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030.

Or. en

Enmienda 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) Los esquemas europeos de certificación en relación con los servicios de seguridad gestionados deben facilitar el uso de estos servicios, en particular a las entidades más pequeñas, como las autoridades locales y regionales o las pymes, que a menudo carecen de la capacidad financiera y humana para

desarrollar estos servicios por sí mismas, pero son vulnerables a ciberataques que pueden tener consecuencias importantes.

Or. en

Enmienda 24
Josianne Cutajar

Propuesta de Reglamento
Considerando 5

Texto de la Comisión	*Enmienda*
(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, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. 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].	(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, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. El ***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 su artículo 67. 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].

Or. en

Enmienda 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Considerando 5

Texto de la Comisión	*Enmienda*
(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, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. 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].	(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 ***y fiabilidad***, 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, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. 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].

Or. en

Enmienda 26
Evžen Tošenovský

Propuesta de Reglamento
Considerando 5

Texto de la Comisión	*Enmienda*
(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, es necesario, por tanto, modificar el Reglamento (UE) 2019/881. 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].	(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 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].

Or. en

Enmienda 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Considerando 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(5 bis) Dado que los esquemas europeos de ciberseguridad deben certificar que los servicios de seguridad gestionados son ofrecidos por personal altamente cualificado, capaz de prestar estos servicios de forma fiable y de garantizar

las normas más estrictas en materia de ciberseguridad, es imperativo que se disponga de suficiente personal altamente cualificado en la Unión. 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. Es importante colmar esta brecha de talento reforzando la cooperación y la coordinación entre las distintas partes interesadas, incluido el sector privado, el mundo académico, los Estados miembros, la Comisión y la ENISA, a fin de aumentar y crear sinergias para la inversión en educación y formación, el desarrollo de colaboraciones público-privadas, el apoyo a las 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. Esto también debe facilitar la movilidad de los profesionales de la ciberseguridad dentro de la Unión.

Or. en

Enmienda 28
Johan Nissinen

Propuesta de Reglamento
Considerando 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(5 bis) Dado que los esquemas de certificación añadirán complejidad a un panorama normativo ya de por sí complejo, es de vital importancia evitar posibles solapamientos o conflictos con las normas y la reglamentación vigentes

en materia de ciberseguridad. Cabe destacar, además, la necesidad de un examen cuidadoso y de proporcionalidad en la aplicación del Reglamento, con el fin de reducir los efectos negativos sobre la libertad de mercado y la innovación.

Or. en

Enmienda 29
Josianne Cutajar

Propuesta de Reglamento
Considerando 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(5 bis) Debe considerarse la posibilidad de contar con una financiación y unos recursos adecuados para realizar las tareas adicionales encomendadas a ENISA por el presente acto.

Or. en

Enmienda 30
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra a – parte introductoria

Texto de la Comisión	*Enmienda*
a) Los puntos 9, 10 y 11 se sustituyen por el texto siguiente:	a) Los puntos ***7,*** 9, 10 y 11 se sustituyen por el texto siguiente:

Or. en

Enmienda 31
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra a

Reglamento (UE) 2019/881
Artículo 2 – punto 7

Texto de la Comisión	*Enmienda*
	7) "gestión de incidentes": la gestión de incidentes según se define en el artículo 6, punto 8, de la Directiva (UE) 2022/2555;

Or. en

Enmienda 32
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra b – parte introductoria

Texto de la Comisión	*Enmienda*
b) Se ***inserta el punto siguiente***:	b) Se ***insertan los puntos siguientes***:

Or. en

Enmienda 33
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra b
Reglamento (UE) 2019/881
Artículo 2 – punto 7 bis

Texto de la Comisión	*Enmienda*
	7 bis) "riesgo": riesgo tal como se define en el artículo 6, punto 9, de la Directiva (UE) 2022/2555;

Or. en

Enmienda 34
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra b
Reglamento (UE) 2019/881
Artículo 2 – punto 14 bis

Texto de la Comisión	*Enmienda*
14 bis) "servicio de seguridad gestionado": servicio ***que consiste en llevar a cabo o prestar asistencia para actividades relacionadas con la gestión*** de ***riesgos de ciberseguridad, en particular, la respuesta a incidentes***, ***las pruebas de penetración***, ***las auditorías*** de ***seguridad y la consultoría***;	14 bis) "servicio de seguridad gestionado": servicio de ***seguridad gestionado en el sentido del artículo 6***, ***punto 40***, de ***la Directiva (UE) 2022/2555***;

Or. en

Enmienda 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra b
Reglamento (UE) 2019/881
Artículo 2 – punto 14 bis

Texto de la Comisión	*Enmienda*
14 bis) "servicio de seguridad gestionado": servicio que consiste en llevar a cabo o prestar asistencia para actividades relacionadas con la gestión de riesgos de ciberseguridad, en particular***,*** la ***respuesta a incidentes***, ***las pruebas de penetración, las auditorías de seguridad y la consultoría***;	14 bis) "servicio de seguridad gestionado": servicio ***gestionado*** que consiste en llevar a cabo o prestar asistencia para actividades relacionadas con la gestión de riesgos de ciberseguridad, en particular la ***prevención, la detección***, ***la respuesta y la recuperación en relación con los incidentes***;

Or. en

Enmienda 36
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 2 – letra b

Reglamento (UE) 2019/881
Artículo 2 – punto 14 bis bis

Texto de la Comisión	*Enmienda*
	14 bis bis) "proveedor de servicios de seguridad gestionados": un proveedor de servicios de seguridad gestionados según se define en el artículo 6, punto 40, de la Directiva (UE) 2022/2555;

Or. en

Enmienda 37
Ville Niinistö
en nombre del Grupo Verts/ALE

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 6
Reglamento (UE) 2019/881
Artículo 47 – apartado 2

Texto de la Comisión	*Enmienda*
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.	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. ***Se incluirán medidas de apoyo para evaluar las necesidades relativas a los trabajadores cualificados, los tipos de capacidades y los itinerarios de formación existentes, así como medidas para colmar las brechas detectadas.***

Or. en

Justificación

El ejercicio de identificación de los productos, servicios y procesos de TIC o de las categorías de estos y de los servicios de seguridad gestionados debe ir acompañado de una evaluación de las capacidades y de medidas para colmar las brechas.

Enmienda 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 6
Reglamento (UE) 2019/881
Artículo 47 – apartado 3 – letra a

Texto de la Comisión	*Enmienda*
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;	a) la disponibilidad y el desarrollo de esquemas nacionales de certificación de la ciberseguridad ***y de normas internacionales y del sector*** 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;

Or. en

Justificación

El programa de trabajo evolutivo de la Unión no solo debe evaluar el desarrollo de los esquemas nacionales, sino también las normas internacionales y del sector.

Enmienda 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 7
Reglamento (UE) 2019/881
Artículo 49 – apartado 7

Texto de la Comisión	*Enmienda*
(7) En el artículo 49, el apartado 7 se sustituye por el texto siguiente:	***suprimido***
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, 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.».

Or. en

Enmienda 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 7
Reglamento (UE) 2019/881
Artículo 49 – apartado 7

Texto de la Comisión	*Enmienda*
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, 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.».***	7. La Comisión, a partir de la propuesta de esquema preparada por ENISA, podrá adoptar actos ***delegados*** 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, 52 y 54. *(Esta modificación se aplica a la totalidad del texto legislativo objeto de examen. Su adopción exigirá las correspondientes adaptaciones técnicas en todo el texto).*

Or. en

Enmienda 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 7
Reglamento (UE) 2019/881
Artículo 49 – apartado 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	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.

Or. en

Enmienda 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 7 bis (nuevo)
Reglamento (UE) 2019/881
Artículo 49 – apartado 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	7 bis) Se inserta el apartado siguiente:
	«7 bis. La Comisión, a partir de la propuesta de esquema preparada por ENISA, podrá adoptar actos delegados que establezcan un esquema europeo de certificación de la ciberseguridad para servicios de seguridad gestionados que cumpla los requisitos de los artículos 51, 52 y 54. Dichos actos delegados se adoptarán de conformidad con el procedimiento a que se refiere el artículo 66 bis.».

Or. en

Enmienda 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 9
Reglamento (UE) 2019/881
Artículo 51 bis – párrafo 1 – letra b

Texto de la Comisión	*Enmienda*
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;	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 ***y fiabilidad*** muy elevado;

Or. en

Enmienda 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 9
Reglamento (UE) 2019/881
Artículo 51 bis – párrafo 1 – letra g

Texto de la Comisión	*Enmienda*
g) garantizar que los productos, servicios y procesos de TIC [y el soporte físico] que se implementen en el contexto de la prestación de los servicios de seguridad gestionados sean seguros por defecto y desde el diseño, no contengan vulnerabilidades conocidas e incluyan las últimas actualizaciones de seguridad.	g) garantizar que los productos, servicios y procesos de TIC [y el soporte físico] que se implementen en el contexto de la prestación de los servicios de seguridad gestionados sean seguros por defecto y desde el diseño, ***se entreguen con un programa informático y un equipo informático actualizados,*** no contengan vulnerabilidades conocidas e incluyan las últimas actualizaciones de seguridad.

Or. en

Enmienda 45
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 9
Reglamento (UE) 2019/881
Artículo 51 bis – párrafo 1 – letra g

Texto de la Comisión	*Enmienda*
g) garantizar que los productos, servicios y procesos de TIC ***[y el soporte físico]*** que se implementen en el contexto de la prestación de los servicios de seguridad gestionados sean seguros por defecto y desde el diseño, no contengan vulnerabilidades conocidas e incluyan las últimas actualizaciones de seguridad.	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, no contengan vulnerabilidades conocidas e incluyan las últimas actualizaciones de seguridad.

Or. en

Enmienda 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 13 – letra b – inciso ii – letra aa
Reglamento (UE) 2019/881
Artículo 56 – apartado 3 – párrafo tercero – letra a

Texto de la Comisión	*Enmienda*
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;	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***, incluidas las pymes. La Comisión velará por que las pymes tengan acceso a un apoyo financiero adecuado***

para la aplicación de las medidas a través de programas de la Unión ya existentes;

Or. en

Enmienda 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 14
Reglamento (UE) 2019/881
Artículo 57 – apartado 1

Texto de la Comisión	*Enmienda*
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.	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***. 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. *(Esta modificación se aplica a la totalidad del texto legislativo objeto de examen. Su adopción exigirá las correspondientes adaptaciones técnicas en todo el texto).*

Or. en

Justificación

Esto refleja la enmienda al artículo 49.

Enmienda 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 16 bis (nuevo)
Reglamento (UE) 2019/881
Artículo 66 bis (nuevo)

Texto de la Comisión	*Enmienda*
	16 bis) Se inserta el artículo siguiente:
	«Artículo 66 bis
	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 bis, se otorgan a la Comisión por un período de cinco años a partir del ... [fecha de entrada en vigor del acto legislativo de base o cualquier otra fecha fijada por los colegisladores]. 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 49, apartado 7 bis, 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 bis, 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.».

Or. en

Enmienda 49
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 17 – parte introductoria
Reglamento (UE) 2019/881
Artículo 67

Texto de la Comisión	*Enmienda*
(17) En el artículo 67, los apartados ***2 y 3*** se sustituyen por el texto siguiente:	17) En el artículo 67, los apartados ***1, 2, 3 y 4*** se sustituyen por el texto siguiente:

Or. en

Enmienda 50
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 17
Reglamento (UE) 2019/881
Artículo 67 – apartado 1

Texto de la Comisión	*Enmienda*
	1. A más tardar el 28 de junio de 2024, y posteriormente cada cuatro años, la Comisión evaluará el impacto, la eficacia y la eficiencia de ENISA y de sus prácticas de trabajo, así como la posible necesidad de modificar su mandato y las repercusiones financieras que tendría la eventual modificación. La evaluación tomará en consideración los comentarios llegados a ENISA en respuesta a sus actividades. Si la Comisión considerara que el funcionamiento continuado de ENISA ha dejado de estar 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.

Or. en

Enmienda 51
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 17
Reglamento (UE) 2019/881
Artículo 67 – apartado 2

Texto de la Comisión	*Enmienda*
2. En la evaluación se analizarán también 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	2. En la evaluación se analizarán también 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.	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***, en particular la evaluación del procedimiento y los plazos previos a la preparación y adopción de los primeros esquemas europeos de certificación de la ciberseguridad y del modo en que podría mejorarse y acelerarse este procedimiento en los esquemas de certificación posteriores***.
	Or. en

Enmienda 52
Evžen Tošenovský

Propuesta de Reglamento
Artículo 1 – párrafo 1 – punto 17
Reglamento (UE) 2019/881
Artículo 67 – apartado 4

Texto de la Comisión	*Enmienda*
	4. A más tardar el 28 de junio de 2024, y posteriormente cada cuatro 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. El informe irá acompañado, cuando sea menester, de una propuesta legislativa.
	Or. en