PARLAMENTO DE GALICIA

BOLETÍN OFICIAL DO **PARLAMENTO DE GALICIA**

X lexislatura
Número 198
23 de outubro de 2017

Fascículo 2

SUMARIO

-10/UECS-000098 (18879)
Consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta do Regulamento do Consello polo que se modifica o Regulamento (UE) nº 904/2010 no que se refire ao suxeito pasivo certificado [COM(2017) 567 final][2017/0248(CNS)] 59219

Resolución da Presidencia, do 18 de outubro de 2017, pola que se admite a trámite o escrito das Cortes Xerais polo que se achega documentación relativa á Proposta de Directiva do Consello pola que se modifica a Directiva 2006/112/CE no que se refire á harmonización e á simplificación de determinadas normas do réxime do imposto sobre o valor engadido e se introduce o réxime definitivo de tributación dos intercambios entre os Estados membros [COM(2017) 596 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017 326 final}

-10/UECS-000099 (18880)
Consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta de Directiva do Consello pola que se modifica a Directiva 2006/112/CE no que se refire á harmonización e á simplificación de determinadas normas do réxime do imposto sobre o valor engadido e se introduce o réxime definitivo de tributación dos intercambios entre os Estados membros [COM(2017) 596 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017 326 final} 59228

4. Informacións e correccións de erros

4.2. Correccións de erros

Corrección de erros no Acordo da Comisión de valoración do concurso para a provisión dos postos de técnico/a de asistencia parlamentaria, técnico/a superior de réxime interior e técnico/a de publicacións do Parlamento de Galicia polo que se fai publica a puntuación provisional acadada polos aspirantes, publicado no BOPG nº 196 do 19 de outubro de 2017 59108

Corrección de erros no acordo da Mesa da Comisión 8ª, Pesca e Marisqueo, de cualificación de emendas ao articulado presentadas ao Proxecto de lei de portos de Galicia 59108

1. Procedementos parlamentarios

1.1. Procedementos de natureza normativa

1.1.2. Propostas de normas

1.1.2.1. Proxectos e proposicións de lei

1.1.2.1.1. Proxectos de lei

Acordo da Mesa do Parlamento, do 20 de outubro de 2017, polo que se amplía o prazo de presentación de emendas ao articulado ao Proxecto de lei de espectáculos públicos e actividades recreativas [(doc. núm. 16854, 10/PL-000006)]

No Rexistro Xeral do Parlamento de Galicia tivo entrada, co número 19086, o escrito do G. P. dos Socialistas de Galicia polo que se solicita a ampliación do prazo para a presentación de emendas ao articulado ao Proxecto de lei de espectáculos públicos e actividades recreativas (doc. núm. 16854, 10/PL-000006).

Visto o disposto no artigo 96 do Regulamento da Cámara, a Mesa, por unanimidade, acorda:

1º. Ampliar, por terceira vez, o prazo de presentación de emendas ao articulado ao Proxecto de lei de espectáculos públicos e actividades recreativas (doc. núm. 16854, 10/PL-000006), ata o día 25 de outubro de 2017 ás 18.30 horas.

2º. Notificar este acordo aos grupos parlamentarios.

3º. Publicar este acordo no *Boletín Oficial do Parlamento de Galicia*.

Santiago de Compostela, 20 de outubro de 2017
Miguel Ángel Santalices Vieira
Presidente

1.1.2.1.5. Proposicións de lei de iniciativa popular

Acordo da Mesa do Parlamento, do 20 de outubro de 2017, polo que se amplía o prazo de presentación de emendas ao articulado á Proposición de lei de iniciativa lexislativa popular de medidas para garantir a enerxía como servizo público e contra a pobreza enerxética [(doc. núm. 37326, 09/PPLI-000013)]

No Rexistro Xeral do Parlamento de Galicia tivo entrada, co número 18983, o escrito do G. P. Popular de Galicia polo que solicita a ampliación do prazo para a presentación de emendas ao articulado á Proposición de lei de iniciativa lexislativa popular de medidas para garantir a enerxía como servizo público e contra a pobreza enerxética (doc. núm. 37326, 09/PPLI-000013).

Visto o disposto no artigo 96 do Regulamento da Cámara, a Mesa, por unanimidade, acorda:

1º. Ampliar, por terceira vez, o prazo de presentación de emendas ao articulado á Proposición de lei de iniciativa lexislativa popular de medidas para garantir a enerxía como servizo público e contra a pobreza enerxética (doc. núm. 37326, 09/PPLI-000013), ata o día 26 de outubro de 2017 ás 18.30 horas.

2º. Notificar este acordo aos grupos parlamentarios.

3º. Publicar este acordo no *Boletín Oficial do Parlamento de Galicia*.

Santiago de Compostela, 20 de outubro de 2017
Miguel Ángel Santalices Vieira
Presidente

1.5. Procedementos relativos a outras institucións e órganos
1.5.4. De ámbito europeo
1.5.4.1. Unión Europea

Resolución da Presidencia, do 18 de outubro de 2017, pola que se admite a trámite o escrito das Cortes Xerais polo que se achega documentación relativa á Proposta de Regulamento do Parlamento Europeo e do Consello relativo a ENISA, a Axencia de Ciberseguridade da UE, e polo que se derroga o Regulamento (UE) nº 526/2013, e relativo á certificación da ciberseguridade das tecnoloxías da información e a comunicación (Regulamento de Ciberseguridade) (Texto pertinente para efectos do EEE) [COM(2017) 477 final] [COM(2017)477 final Anexo] [2017/0225 (COD)]{SWD(2017) 500final}{SWD(2017)501 final}{SWD(2017)502 final}

-10/UECS-000097 (18844)
Consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta de Regulamento do Parlamento Europeo e do Consello relativo a ENISA, a Axencia de Ciberseguridade da UE, e polo que se derroga o Regulamento (UE) nº 526/2013, e relativo á certificación da ciberseguridade das tecnoloxías da información e a comunicación (Regulamento de Ciberseguridade) (Texto pertinente a efectos do EEE) [COM(2017) 477 final] [COM(2017)477 final Anexo] [2017/0225 (COD)]{SWD(2017) 500final}{SWD(2017)501 final}{SWD(2017)502 final}

No Rexistro Xeral do Parlamento de Galicia tivo entrada, co número 18844, o escrito das Cortes Xerais polo que se achega documentación relativa á solicitude da Comisión Mixta para la Unión Europea en relación coa consulta sobre aplicación do principio de subsidiariedade relativo á Proposta de Regulamento do Parlamento Europeo e do Consello relativo a ENISA, a Axencia de Ciberseguridade da UE, e polo que se deroga o Regulamento (UE) nº 526/2013, e relativo á certificación da ciberseguridade das tecnoloxías da información e a comunicación (Regulamento de Ciberseguridade) (Texto pertinente para efectos do EEE) [COM(2017) 477 final] [COM(2017)477 final Anexo] [2017/0225 (COD)]{SWD(2017) 500final}{SWD(2017)501 final}{SWD(2017)502 final}

Conforme o establecido na norma segunda das Normas reguladoras do procedemento para o control do principio de subsidiariedade nos proxectos lexislativos da Unión Europea (BOPG 27 do 9 de decembro de 2016), resolvo:

1º. Trasladarlles o referido escrito á Comisión 6ª, Industria, Enerxía, Comercio e Turismo, e mais aos portavoces dos grupos parlamentarios e ordenar a súa publicación no *Boletín Oficial do Parlamento de Galicia.*

2º. Conforme o disposto na norma terceira das citadas normas, no prazo dos dez días naturais seguintes á remisión do proxecto de acto lexislativo, os grupos parlamentarios poderán presentar propostas de ditame motivado nas que deberán expoñer as razóns polas que consideran que o proxecto de acto lexislativo da Unión Europea resulta contrario, en todo ou en parte, ao principio de subsidiariedade.

As propostas de ditame motivado presentaranse ante a Mesa, que as cualificará e admitirá a trámite se reúnen os requisitos establecidos neste acordo.

A ausencia de propostas de ditame determinará a finalización do procedemento.

3º. Dar conta desta resolución na próxima reunión da Mesa que teña lugar.

Santiago de Compostela, 18 de outubro de 2017
Miguel Ángel Santalices Vieira
Presidente

Resolución da Presidencia, do 18 de outubro de 2017, pola que se admite a trámite o escrito das Cortes Xerais polo que se achega documentación relativa á Proposta do Regulamento do Consello polo que se modifica o Regulamento (UE) nº 904/2010 no que se refire ao suxeito pasivo certificado [COM(2017) 567 final][2017/0248(CNS)]

-10/UECS-000098 (18879)
Consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta do Regulamento do Consello polo que se modifica o Regulamento (UE) nº 904/2010 no que se refire ao suxeito pasivo certificado [COM(2017) 567 final][2017/0248(CNS)]

No Rexistro Xeral do Parlamento de Galicia tivo entrada, co número 18879, o escrito das Cortes Xerais polo que se achega documentación relativa á solicitude da Comisión Mixta para a Unión Europea en relación coa consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta do Regulamento do Consello polo que se modifica o Regulamento (UE) nº 904/2010 no que se refire ao suxeito pasivo certificado [COM(2017) 567 final][2017/0248(CNS)]

Conforme o establecido na norma segunda das Normas reguladoras do procedemento para o control do principio de subsidiariedade nos proxectos lexislativos da Unión Europea (BOPG 27 do 9 de decembro de 2016), resolvo:

1º. Trasladarlles o referido escrito á Comisión 3ª, Economía, Facenda e Orzamentos, e mais aos portavoces dos grupos parlamentarios e ordenar a súa publicación no *Boletín Oficial do Parlamento de Galicia.*

2º. Conforme o disposto na norma terceira das citadas normas, no prazo dos dez días naturais seguintes á remisión do proxecto de acto lexislativo, os grupos parlamentarios poderán presentar propostas de ditame motivado nas que deberán expoñer as razóns polas que consideran que o proxecto de acto lexislativo da Unión Europea resulta contrario, en todo ou en parte, ao principio de subsidiariedade.

As propostas de ditame motivado presentaranse ante a Mesa, que as cualificará e admitirá a trámite se reúnen os requisitos establecidos neste acordo.

A ausencia de propostas de ditame determinará a finalización do procedemento.

3º. Dar conta desta resolución na próxima reunión da Mesa que teña lugar.

Santiago de Compostela, 18 de outubro de 2017
Miguel Ángel Santalices Vieira
Presidente

Resolución da Presidencia, do 18 de outubro de 2017, pola que se admite a trámite o escrito das Cortes Xerais polo que se achega documentación relativa á Proposta de Directiva do Consello pola que se modifica a Directiva 2006/112/CE no que se refire á harmonización e á simplificación de determinadas normas do réxime do imposto sobre o valor engadido e se introduce o réxime definitivo de tributación dos intercambios entre os Estados membros [COM(2017) 596 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017 326 final}

-10/UECS-000099 (18880)
Consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta de Directiva do Consello pola que se modifica a Directiva 2006/112/CE no que se refire á harmonización e á simplificación de determinadas normas do réxime do imposto sobre o valor engadido e se introduce o réxime definitivo de tributación dos intercambios entre os Estados membros [COM(2017) 596 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017 326 final}

No Rexistro Xeral do Parlamento de Galicia tivo entrada, co número 18880, o escrito das Cortes Xerais polo que se achega documentación relativa á solicitude da Comisión Mixta para a Unión Europea en relación coa consulta sobre a aplicación do principio de subsidiariedade relativo á Proposta de Directiva do Consello pola que se modifica a Directiva 2006/112/CE no que se refire á harmonización e á simplificación de determinadas normas do réxime do imposto sobre o valor engadido e se introduce o réxime definitivo de tributación dos intercambios entre os Estados membros [COM(2017) 596 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017 326 final}

Conforme o establecido na norma segunda das Normas reguladoras do procedemento para o control do principio de subsidiariedade nos proxectos lexislativos da Unión Europea (BOPG 27 do 9 de decembro de 2016), resolvo:

1º. Trasladarlles o referido escrito á Comisión 3ª, Economía, Facenda e Orzamentos, e mais aos portavoces dos grupos parlamentarios e ordenar a súa publicación no *Boletín Oficial do Parlamento de Galicia.*

2º. Conforme o disposto na norma terceira das citadas normas, no prazo dos dez días naturais seguintes á remisión do proxecto de acto lexislativo, os grupos parlamentarios poderán presentar propostas de ditame motivado nas que deberán expoñer as razóns polas que consideran que o proxecto de acto lexislativo da Unión Europea resulta contrario, en todo ou en parte, ao principio de subsidiariedade.

As propostas de ditame motivado presentaranse ante a Mesa, que as cualificará e admitirá a trámite se reúnen os requisitos establecidos neste acordo.

A ausencia de propostas de ditame determinará a finalización do procedemento.

3º. Dar conta desta resolución na próxima reunión da Mesa que teña lugar.

Santiago de Compostela, 18 de outubro de 2017
Miguel Ángel Santalices Vieira
Presidente

4. Informacións e correccións de erros

4.2. Correccións de erros

Corrección de erros no Acordo da Comisión de valoración do concurso para a provisión dos postos de técnico/a de asistencia parlamentaria, técnico/a superior de réxime interior e técnico/a de publicacións do Parlamento de Galicia polo que se fai publica a puntuación provisional acadada polos aspirantes, publicado no BOPG nº 196 do 19 de outubro de 2017

Advertido un erro no anexo de puntuación do Acordo da Comisión de valoración do concurso para a provisión dos postos de técnico/a de asistencia parlamentaria, técnico/a superior de réxime interior e técnico/a de publicacións do Parlamento de Galicia, polo que se fai publica a puntuación provisional acadada polos aspirantes, no apartado relativo ao posto: técnico/a de asistencia parlamentaria, no aspirante Martín Nercellas Méndez a puntuación asignada para o mérito 6f) debe figurar no mérito 6e).

Santiago de Compostela, 20 de outubro de 2017
Carolina Costoya Pardo
Presidenta da Comisión de valoración

Corrección de erros no acordo da Mesa da Comisión 8ª, Pesca e Marisqueo, de cualificación de emendas ao articulado presentadas ao Proxecto de lei de portos de Galicia

Advertido un erro material no acordo da Mesa da Comisión 8ª, Pesca e Marisqueo, de cualificación de emendas ao articulado presentadas ao Proxecto de lei de portos de Galicia, publicado no Boletín Oficial do Parlamento de Galicia núm. 196, do 19 de outubro de 2017, procédese á súa corrección nos seguintes termos:

No sumario e mais na páxina 58064, onde di:

«Emendas ao articulado:

— Do G. P. Popular de Galicia, 2 emendas (doc. núm. 18164)
— Do G. P. de En Marea, 53 emendas (doc. núm. 18234)
— Do G. P. dos Socialistas de Galicia, 177 emendas (doc. núm. 18235)
— Do G. P. Popular de Galicia, 106 emendas (doc. núm. 18236 e correccion de erros no doc. 18291)»

Debe dicir:

«Emendas ao articulado:

— Do G. P. Popular de Galicia, 2 emendas (doc. núm. 18164)
— Do G.P. de En Marea, 53 emendas (doc. núm. 18234)
— Do G. P. dos Socialistas de Galicia, 177 emendas (doc. núm. 18235)
— Do G. P. do Bloque Nacionalista Galego, 106 emendas (doc. núm. 18236 e correccion de erros no doc. 18291)»

Santiago de Compostela, 23 de outubro 2017
Xosé Antón Sarmiento Méndez
Letrado oficial maior

- Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad») (Texto pertinente a efectos del EEE) **[COM(2017) 477 final]** [COM(2017) 477 final Anexo] [2017/0225 (COD)] {SWD(2017) 500 final} {SWD(2017) 501 final} {SWD(2017) 502 final}

COMISIÓN
EUROPEA

Bruselas, 13.9.2017
COM(2017) 477 final

ANNEX 1

ANEXO

DE LA

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

REQUISITOS QUE DEBEN CUMPLIR LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD

Los organismos de evaluación de la conformidad que deseen ser acreditados deberán cumplir los siguientes requisitos:

1. El organismo de evaluación de la conformidad se establecerá de conformidad con el Derecho interno y tendrá personalidad jurídica.

2. El organismo de evaluación de la conformidad será un organismo tercero independiente de la organización o de los productos y servicios de TIC que evalúa.

3. Podrá tratarse de un organismo perteneciente a una asociación empresarial o una federación profesional que represente a las empresas que participan en el diseño, la fabricación, el suministro, el montaje, el uso o el mantenimiento de los productos o servicios de TIC que evalúa, a condición de que se demuestre su independencia y la ausencia de conflictos de intereses.

4. El organismo de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no serán el diseñador, el fabricante, el proveedor, el instalador, el comprador, el propietario, el usuario ni el encargado del mantenimiento del producto o servicio de TIC que debe evaluarse, ni tampoco el representante autorizado de ninguno de ellos. Ello no será óbice para que se utilicen los productos evaluados necesarios para las actividades del organismo de evaluación de la conformidad o para que se utilicen dichos productos para fines personales.

5. El organismo de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, la fabricación o construcción, la comercialización, la instalación, el uso o el mantenimiento de los productos o servicios de TIC, ni representarán a las partes que participan en estas actividades. 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. Ello se aplicará, en particular, a los servicios de consultoría.

6. 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.

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

8. El organismo de evaluación de la conformidad deberá ser capaz de llevar a cabo todas las tareas de evaluación de la conformidad que le hayan sido asignadas en virtud del presente Reglamento, tanto si dichas tareas las efectúa el propio organismo como si se realizan en su nombre y bajo su responsabilidad.

9. En todo momento, respecto a cada procedimiento de evaluación de la conformidad y cada tipo, categoría o subcategoría de producto o servicio de TIC, el organismo de evaluación de la conformidad dispondrá:

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

b) de las descripciones necesarias de los procedimientos con arreglo a los cuales se efectúa la evaluación de la conformidad, garantizando la transparencia y la posibilidad de reproducción de estos procedimientos; dispondrá asimismo de las políticas y procedimientos adecuados que permitan distinguir entre las tareas efectuadas en tanto que organismo notificado y cualquier otra actividad;

c) de los procedimientos necesarios para desempeñar sus actividades teniendo debidamente en cuenta el tamaño de una empresa, el sector en que opera, su estructura, el grado de complejidad de la tecnología del producto o servicio de TIC de que se trate y si el proceso de producción es en serie.

10. El organismo de evaluación de la conformidad dispondrá de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrá acceso a todos los equipos e instalaciones que necesite.

11. El personal que efectúe las actividades de evaluación de la conformidad tendrá:

a) una sólida formación técnica y profesional referida a todas las actividades de evaluación de la conformidad;

b) un conocimiento satisfactorio de los requisitos de las evaluaciones que efectúe y la autoridad apropiada para efectuar tales evaluaciones;

c) un conocimiento y una comprensión adecuados de los requisitos y normas de ensayo aplicables;

d) la capacidad necesaria para elaborar certificados, documentos e informes que demuestren que se han efectuado las evaluaciones.

12. Se garantizará la imparcialidad del organismo de evaluación de la conformidad, de sus máximos directivos y de su personal de evaluación.

13. La remuneración de los máximos directivos y del personal de evaluación del organismo de evaluación de la conformidad no dependerá del número de evaluaciones que efectúe ni de los resultados de dichas evaluaciones.

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

15. El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información obtenida en el marco de las tareas realizadas con arreglo al presente Reglamento o a cualquier disposición de Derecho nacional por la que se aplique, salvo con respecto a las autoridades competentes de los Estados miembros en que realice sus actividades.

16. Los organismos de evaluación de la conformidad cumplirán los requisitos de la norma EN ISO/IEC 17065:2012.

17. 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 EN ISO/IEC 17025:2005.

COMISIÓN
EUROPEA

Bruselas, 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

(Texto pertinente a efectos del EEE)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La Unión Europea ha adoptado una serie de medidas para incrementar la resiliencia y mejorar su preparación en materia de ciberseguridad. La primera Estrategia de Ciberseguridad de la UE[1], adoptada en 2013, estableció objetivos estratégicos y acciones concretas para mejorar la resiliencia, reducir la ciberdelincuencia, desarrollar políticas y capacidades en materia de ciberdefensa, desarrollar recursos industriales y tecnológicos y establecer una política coherente del ciberespacio internacional para la UE. En este contexto, se han producido desde entonces acontecimientos importantes, en particular el segundo mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[2] y la adopción de la **Directiva sobre seguridad de las redes y los sistemas de información**[3] (en lo sucesivo, «Directiva SRI»), que constituyen la base de la presente propuesta.

Por otra parte, en **2016 la Comisión Europea adoptó la Comunicación «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora»**[4], en la que se anunciaron nuevas medidas para intensificar la cooperación, la información y la puesta en común de conocimientos y para incrementar la resiliencia y preparación de la UE, teniendo también en cuenta la perspectiva de incidentes a gran escala y una posible crisis paneuropea de ciberseguridad. En este contexto, la Comisión anunció que presentaría la **evaluación** y **revisión** del Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo relativo a ENISA y por el que se deroga el Reglamento (CE) n.º 460/2004 (el «Reglamento de ENISA»). El proceso de evaluación podría conducir a una posible reforma de la Agencia y a un reforzamiento de sus facultades y capacidades para apoyar a los Estados miembros de manera sostenible. Le conferiría, por tanto, un papel más operativo y central para lograr la resiliencia en materia de ciberseguridad y reconocería en su nuevo mandato las nuevas responsabilidades de la Agencia en virtud de la Directiva SRI.

La Directiva SRI representa un primer paso esencial con vistas a fomentar una cultura de gestión de riesgos, al introducir requisitos de seguridad como obligaciones legales de los agentes económicos clave, en particular los operadores que prestan servicios esenciales (operadores de servicios esenciales u OSE) y los proveedores de algunos servicios digitales clave (proveedores de servicios digitales o PSE). Dado que los requisitos de seguridad se consideran esenciales para salvaguardar los beneficios de la digitalización de la sociedad en curso, y vista la rápida proliferación de dispositivos conectados (la «internet de las cosas»), la Comunicación de 2016 también proponía la idea de crear un marco para la certificación de seguridad de los productos y servicios de TIC a fin de incrementar la confianza y la seguridad en el mercado único digital. La certificación de ciberseguridad de las TIC adquiere particular importancia teniendo en cuenta el creciente uso de tecnologías que requieren un elevado nivel

---

1 Comunicación conjunta de la Comisión Europea y el Servicio Europeo de Acción Exterior: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», JOIN(2013).

2 Reglamento (UE) n.º 526/2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004

3 Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

4 Comunicación de la Comisión «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora» (COM/2016/410 final).

de ciberseguridad, como los automóviles conectados y automatizados, la sanidad electrónica o los sistemas de control de automatización industrial (IACS).

Estas medidas y anuncios políticos quedaron aún más reforzados tras las **conclusiones del Consejo** de 2016, que reconocían que «las ciberamenazas y las vulnerabilidades siguen evolucionando e intensificándose, lo cual requerirá una cooperación continuada y más estrecha, sobre todo a la hora de dar respuesta a incidentes de ciberseguridad transfronterizos y de gran envergadura». Dichas conclusiones reafirmaban que «el Reglamento ENISA es uno de los elementos básicos del marco de la UE sobre ciberresiliencia»[5] y pedían a la Comisión que tomase nuevas medidas para abordar la cuestión de la certificación a nivel europeo.

El establecimiento de un sistema de certificación exigiría la implantación de un sistema de gobernanza adecuado a nivel de la UE, entre otras cosas gracias a los conocimientos aportados por una agencia de la UE independiente. A este respecto, la presente propuesta señala a ENISA como el organismo natural a nivel de la UE competente para la ciberseguridad que debería asumir esa función para reunir a los organismos nacionales competentes en materia de certificación y coordinar su trabajo.

En su Comunicación sobre la **revisión intermedia de la Estrategia para el Mercado Único Digital de mayo de 2017**, la Comisión especificó además que, a más tardar en septiembre de 2017, revisaría el mandato de ENISA. Se trataría de definir su papel en el cambiante ecosistema de la ciberseguridad y de desarrollar medidas relativas a normas, certificación y etiquetado de ciberseguridad para aumentar la ciberseguridad de los sistemas basados en las TIC, incluidos los objetos conectados[6]. Las **conclusiones del Consejo Europeo** de junio de 2017[7] saludaron la intención de la Comisión de revisar la estrategia de ciberseguridad en septiembre y de proponer nuevas acciones específicas antes de finalizar 2017.

La propuesta de Reglamento establece un conjunto completo de medidas que se basan en actuaciones anteriores y fomentan objetivos específicos que se refuerzan mutuamente:

- aumentar **las capacidades y la preparación** de los Estados miembros y de las empresas;
- mejorar **la cooperación y la coordinación** entre los Estados miembros y las instituciones, órganos y organismos de la UE;
- aumentar **las capacidades a nivel de la UE para complementar la acción de los Estados miembros**, en particular en caso de cibercrisis transfronteriza;
- aumentar **la sensibilización** de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad;
- aumentar en general **la transparencia de la garantía de ciberseguridad**[8] de los productos y servicios de TIC, a fin de reforzar la confianza en el mercado único digital y en la innovación digital; y

---

5 Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

6 Comunicación de la Comisión relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, COM(2017) 228.

7 Reunión del Consejo Europeo (22 y 23 de junio de 2017): Conclusiones EUCO 8/17.

8 La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información suficiente sobre las propiedades de ciberseguridad para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

- evitar **la fragmentación de los sistemas de certificación** en la UE y de los requisitos de seguridad y criterios de evaluación conexos en los distintos Estados miembros y sectores.

La siguiente sección de la exposición de motivos explica con más detalle la justificación de la iniciativa con respecto a las acciones propuestas para ENISA y la certificación de ciberseguridad.

ENISA

ENISA actúa como centro de conocimientos especializados para mejorar la seguridad de las redes y de la información en la Unión y apoyar la creación de capacidades en los Estados miembros.

ENISA se creó en 2004[9] con el fin de contribuir al objetivo general de garantizar un elevado nivel de seguridad de las redes y de la información en la UE. En 2013, el Reglamento (UE) n.º 526/2013 estableció el nuevo mandato de la Agencia para un período de siete años, hasta 2020. La Agencia tiene sus oficinas en Grecia, en particular con sede administrativa en Heraklion (Creta) y operaciones principales en Atenas.

ENISA es una agencia pequeña, cuyo presupuesto y efectivos son bajos en comparación con todas las agencias de la UE. Su mandato es de duración determinada.

ENISA asiste a las instituciones europeas, los Estados miembros y la comunidad empresarial a la hora de **abordar, dar respuesta y especialmente prevenir los problemas de seguridad de las redes y de la información**. Lo hace a través de una serie de actividades en los cinco ámbitos enunciados en su estrategia[10]:

- Asesoramiento: suministro de información y asesoramiento sobre las principales cuestiones de seguridad de las redes y de la información.
- Política: apoyo a la elaboración y aplicación de políticas en la Unión.
- Capacidad: apoyo a la creación de capacidad en la Unión (por ejemplo, mediante formación, recomendaciones y actividades de sensibilización).
- Comunidad: impulsar al colectivo de la seguridad de las redes y de la información (por ejemplo, apoyo a los equipos de respuesta a emergencias informáticas o CERT, o coordinación de ciberejercicios paneuropeos).
- Facilitación (por ejemplo, contactos con las partes interesadas y relaciones internacionales).

En el curso de las negociaciones de la Directiva SRI, los colegisladores de la UE decidieron asignar importantes funciones a ENISA a la hora de aplicar dicha Directiva. En particular, la Agencia se encarga de la secretaría de la red de CSIRT (establecida para promover la cooperación operativa rápida y eficaz entre los Estados miembros sobre incidentes de ciberseguridad específicos y compartir información sobre riesgos), y también debe prestar asistencia al Grupo de cooperación en la ejecución de sus tareas. Además, la Directiva exige a

[9] Reglamento (CE) n.º 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

[10] https://www.enisa.europa.eu/publications/corporate/enisa-strategy

ENISA que preste asistencia a los Estados miembros y a la Comisión ofreciéndoles sus conocimientos y asesoramiento y facilitando el intercambio de las mejores prácticas.

De conformidad con el Reglamento de ENISA, la Comisión ha llevado a cabo una evaluación de la Agencia, que incluye un estudio independiente, así como una consulta pública. La evaluación se centró en la pertinencia, repercusión, eficacia, eficiencia, coherencia y valor añadido europeo de la Agencia en lo que se refiere a su rendimiento, gobernanza, estructura organizativa interna y prácticas de trabajo durante el período 2013-2016.

El rendimiento global de ENISA fue evaluado positivamente por la mayoría de quienes respondieron[11] (74 %) a la consulta pública. También fue mayoritaria la opinión de que ENISA estaba alcanzando sus diferentes objetivos (al menos un 63 % para cada uno de los objetivos). Los servicios y productos de ENISA son utilizados de forma regular (mensualmente o con mayor frecuencia) por casi la mitad de quienes respondieron (46 %) y apreciados por el hecho de proceder de un organismo a nivel de la UE (83 %) y por su calidad (62 %).

No obstante, una gran mayoría (88 %) de las respuestas consideraba que los actuales instrumentos y mecanismos disponibles a nivel de la UE son insuficientes o solo parcialmente adecuados para hacer frente a los actuales desafíos en materia de ciberseguridad. Una gran mayoría de las respuestas (98 %) indicaba que un organismo de la UE debía abordar estas necesidades y, entre ellos, al 99 % ENISA le parecía la organización adecuada para ello. Además, el 67,5 % de las respuestas expresó la opinión de que ENISA podría desempeñar algún papel en el establecimiento de un marco armonizado para la certificación de seguridad de los productos y servicios de TI.

La evaluación global (sobre la base no solo de la consulta pública, sino también de una serie de entrevistas personales, encuestas específicas adicionales y seminarios) llegó a las siguientes conclusiones:

- Los objetivos de ENISA siguen siendo pertinentes en la actualidad. En un contexto de rápida evolución tecnológica y de amenazas cambiantes, y visto que los riesgos globales relacionados con la ciberseguridad son cada vez mayores, existe una clara necesidad en la UE de fomentar y seguir reforzando los conocimientos técnicos de alto nivel sobre cuestiones de ciberseguridad. Deben crearse en los Estados miembros capacidades que permitan comprender y responder a las amenazas, y es precisa una cooperación de las partes interesadas en todos los ámbitos temáticos e instituciones.
- A pesar de su reducido presupuesto, la Agencia ha sido operativamente eficiente en la utilización de sus recursos y en el desempeño de sus funciones. La existencia de dos sedes en Atenas y Heraklion, no obstante, ha generado también costes administrativos suplementarios.
- En cuanto a eficacia, ENISA ha alcanzado parcialmente sus objetivos. La Agencia ha contribuido satisfactoriamente a la mejora de la seguridad de las redes y de la información en Europa merced a la oferta de creación de capacidad en 28 Estados

[11] Noventa partes interesadas procedentes de 19 Estados miembros respondieron a la consulta (88 respuestas y 2 documentos de posición), incluidas las autoridades nacionales de 15 Estados miembros y 8 organizaciones representativas de un número importante de empresas europeas.

miembros[12], mejorando la cooperación entre los Estados miembros y las partes interesadas de la seguridad de las redes y de la información y facilitando asesoramiento, creando comunidades y apoyando la formulación de políticas. Globalmente, ENISA se ha centrado diligentemente en la ejecución de su programa de trabajo y ha actuado como socio fiable de las partes interesadas, en un ámbito cuya acusada importancia transfronteriza ha sido reconocida solo recientemente.

- ENISA consiguió dejar su huella, al menos en cierta medida, en el amplio campo de la seguridad de las redes y de la información, pero no ha conseguido plenamente desarrollar una imagen sólida ni obtener visibilidad suficiente para ser reconocida como «el» centro de conocimientos especializados en Europa. La explicación reside en la amplitud de su mandato, que no iba acompañado de unos recursos proporcionalmente suficientes. Además, ENISA es la única agencia de la UE cuyo mandato es de duración determinada, lo que limita su capacidad para desarrollar una visión a largo plazo y apoyar a sus partes interesadas de manera sostenible. Esto contrasta también con las disposiciones de la Directiva SRI, que atribuye a ENISA tareas sin señalar fecha de finalización. Por último, la evaluación constató que esta limitada eficacia puede explicarse en parte por la fuerte dependencia de asesoramiento externo con preferencia al interno y por las dificultades para contratar y retener personal especializado.
- La última, pero no menos importante, conclusión de la evaluación es que el valor añadido de ENISA radica principalmente en su capacidad para potenciar la cooperación sobre todo entre los Estados miembros, y especialmente con los colectivos interesados en la seguridad de las redes y de la información (en particular entre los CSIRT). No existe nadie a nivel de la UE que preste apoyo a una gama tan amplia de partes interesadas en la seguridad de las redes y de la información. No obstante, debido a la necesidad de priorizar estrictamente sus actividades, el programa de trabajo de ENISA lo definen principalmente las necesidades de los Estados miembros. En consecuencia, no responde suficientemente a las de otras partes interesadas, en particular la industria. Además, esto hizo que la Agencia tratara de satisfacer las necesidades de sus interlocutores clave, lo que le impidió alcanzar un impacto mayor. Por lo tanto, el valor añadido aportado por la Agencia fue distinto según las necesidades divergentes de sus partes interesadas y la medida en que la Agencia pudo responder a ellas (por ejemplo, grandes frente a pequeños Estados miembros; Estados miembros frente a la industria).

En resumen, los resultados de las consultas con las partes interesadas y de la evaluación sugirieron la necesidad de adaptar los recursos y el mandato de ENISA para que pueda desempeñar un papel adecuado en la respuesta a los retos actuales y futuros.

[12] Se pidió a quienes respondieron a la consulta pública que indicaran cuáles consideraban las principales logros de ENISA durante el período 2013-2016. Respuestas procedentes de todos los grupos (55 en total, incluidas 13 de autoridades nacionales, 20 del sector privado y 22 de «otros») percibieron los siguientes logros principales de ENISA: 1) la coordinación de los ejercicios de Cyber Europe; 2) la prestación de apoyo a los CERT/CSIRT a través de cursos de formación y seminarios para fomentar la coordinación y el intercambio; 3) las publicaciones de ENISA (directrices y recomendaciones, informes sobre la perspectiva de amenazas, estrategias para la notificación de incidentes y la gestión de crisis, etc.) que se consideraron útiles tanto para crear y actualizar los marcos nacionales de seguridad como para servir de referencia a los responsables de la formulación de políticas y a los profesionales de la ciberseguridad; 4) la contribución a la promoción de la Directiva SRI; 5) los esfuerzos destinados a aumentar la sensibilización a través del mes de la ciberseguridad.

Habida cuenta de estos resultados, la presente propuesta revisa el actual mandato de ENISA y establece un nuevo conjunto de tareas y funciones, con vistas a apoyar de manera efectiva y eficaz los esfuerzos de los Estados miembros, las instituciones de la UE y otras partes interesadas para garantizar la seguridad del ciberespacio en la Unión Europea. El nuevo mandato propuesto pretende atribuir a la Agencia funciones más sólidas y centrales, en particular respaldando también a los Estados miembros a la hora de aplicar la Directiva SRI y hacer frente a amenazas específicas de manera más activa (capacidad operativa), y convirtiéndose en un centro de conocimientos especializados que asista a los Estados miembros y la Comisión en el ámbito de la certificación de la ciberseguridad. En virtud de la presente propuesta:

- ENISA recibiría un mandato permanente que le proporcionaría una base estable para el futuro. El mandato, los objetivos y las funciones deberían seguir sujetos a revisión periódica.
- El mandato propuesto aclara en mayor medida el papel de ENISA como agencia de la UE para la ciberseguridad y como punto de referencia en el ecosistema de ciberseguridad de la UE, actuando en estrecha cooperación con todos los demás organismos pertinentes de dicho ecosistema.
- La organización y la gobernanza de la Agencia, que se consideraron positivas en la evaluación, serían moderadamente revisadas, en particular para cerciorarse de que queden mejor reflejadas en su trabajo las necesidades de la comunidad de partes interesadas en general.
- Se delinea el alcance propuesto del mandato, que refuerza los ámbitos en los que la Agencia ha mostrado un claro valor añadido y añade otros nuevos en los que se necesita apoyo a la vista de los nuevos instrumentos y prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el inminente plan director de ciberseguridad de la UE para la cooperación en caso de cibercrisis y la certificación de seguridad de las TIC.
    - **Formulación y ejecución de las políticas de la UE:** ENISA se encargaría de contribuir proactivamente a la elaboración de políticas en el ámbito de la seguridad de las redes y la información, así como a otras iniciativas políticas con elementos de ciberseguridad en los distintos sectores (como energía, transporte o finanzas). Para ello, debería poseer un sólido papel consultivo, que podría desempeñar aportando dictámenes independientes y trabajos preparatorios para el desarrollo y la actualización de las políticas y la legislación. ENISA también prestaría apoyo a las políticas y la legislación de la UE en el ámbito de las comunicaciones electrónicas, la identidad electrónica y los servicios de confianza, con vistas a promover un mayor nivel de ciberseguridad. En la fase de aplicación, en particular en el contexto del Grupo de cooperación de la SRI, ENISA asistiría a los Estados miembros en la consecución de un planteamiento coherente sobre la aplicación de la Directiva SRI a través de fronteras y sectores, así como en otras leyes y políticas pertinentes. A fin de sostener la revisión periódica de las políticas y la legislación en el ámbito de la ciberseguridad, ENISA proporcionaría también informes periódicos sobre el estado de la aplicación del marco jurídico de la UE.
    - **Creación de capacidades:** ENISA contribuiría a la mejora de las capacidades y conocimientos técnicos de las autoridades públicas nacionales y de la UE, en particular en lo que se refiere a la respuesta a incidentes y a la supervisión de

las medidas reglamentarias relacionadas con la ciberseguridad. La Agencia también debería contribuir al establecimiento de los centros de puesta en común y análisis de la información (ISACS) en diversos sectores, aportando mejores prácticas y orientaciones sobre los procedimientos e instrumentos disponibles, así como abordando adecuadamente las cuestiones reglamentarias relacionadas con el intercambio de información.

- **Conocimientos e información, sensibilización:** ENISA se convertiría en la plataforma de información de la UE. Esto implicaría la promoción y el intercambio de las mejores prácticas e iniciativas en toda la UE mediante la puesta en común de información sobre ciberseguridad procedente de las instituciones, órganos y organismos nacionales y de la UE. La Agencia facilitaría asimismo asesoramiento, orientación y mejores prácticas sobre la seguridad de las infraestructuras críticas. Tras un incidente transfronterizo de ciberseguridad importante, ENISA elaboraría también informes con el fin de ofrecer orientaciones a las empresas y los ciudadanos de toda la UE. Esta línea de trabajo implicaría también la organización periódica de actividades de sensibilización, en coordinación con las autoridades de los Estados miembros.

- **Tareas relacionadas con el mercado (normalización, certificación de la ciberseguridad):** ENISA desempeñaría una serie de funciones específicas de apoyo del mercado interior, incluido un «observatorio del mercado» de la ciberseguridad, analizando las tendencias pertinentes en el mercado de la ciberseguridad para adecuar mejor la oferta y la demanda, y respaldando el desarrollo de las políticas de la UE en los ámbitos de la normalización de las TIC y la certificación de ciberseguridad de las TIC. En particular, en relación con la normalización, facilitaría el establecimiento y la adopción de normas de ciberseguridad. ENISA también ejecutaría las tareas previstas en el contexto del futuro marco de certificación (véase la sección siguiente).

- **Investigación e innovación:** ENISA aportaría sus conocimientos técnicos asesorando a las autoridades nacionales y de la UE sobre la fijación de prioridades de investigación y desarrollo, especialmente en el contexto de la asociación público-privada contractual (APPc) sobre ciberseguridad. Las recomendaciones de ENISA en materia de investigación se trasladarían al nuevo Centro Europeo de Investigación y Competencias sobre Ciberseguridad en virtud del próximo marco financiero plurianual. ENISA también participaría, previa solicitud de la Comisión, en la ejecución de los programas de financiación de la investigación y la innovación. de la UE.

- **Cooperación operativa y gestión de crisis:** Esta línea de trabajo debería reforzar las capacidades operativas preventivas existentes, especialmente potenciando los ejercicios paneuropeos en la materia (Cyber Europe) para que se celebren anualmente, y facilitar la cooperación operativa en tanto que secretaría de la red de CSIRT (con arreglo a la Directiva SRI), garantizando, entre otras cosas, el buen funcionamiento de la infraestructura de TI y de los canales de comunicación de la mencionada red. En este contexto, resultaría necesaria una cooperación estructurada con el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) y otros organismos pertinentes de la UE. Además, una cooperación estructurada con el CERT-UE, en estrecha proximidad física, debería desembocar en una función que facilitase asistencia técnica en caso de incidentes significativos y apoyase el análisis de incidentes. Los Estados miembros de la UE que la solicitasen recibirían asistencia para gestionar

incidentes y apoyo para el análisis de vulnerabilidades, artefactos e incidentes a fin de reforzar su propia capacidad de prevención y respuesta.

- ENISA también intervendría en el **plan director de ciberseguridad de la UE** presentado en el marco de este conjunto de medidas y que contiene la recomendación de la Comisión a los Estados miembros para dar una respuesta coordinada a los incidentes y crisis de ciberseguridad de gran escala y carácter transfronterizo a nivel de la UE[13]. ENISA facilitaría la cooperación entre Estados miembros concretos en la gestión de la respuesta de emergencia mediante el análisis y la agregación de los informes de situación nacionales sobre la base de la información que los Estados miembros y otras entidades pongan a disposición de la Agencia de forma voluntaria.

- **Certificación de la ciberseguridad de los productos y servicios de TIC**

A fin de establecer y preservar la confianza y la seguridad, es preciso que los productos y servicios de TIC incorporen directamente las características de seguridad en las etapas iniciales de su diseño y desarrollo técnicos (seguridad a través del diseño). Por otra parte, los clientes y usuarios necesitan poder comprobar el nivel de garantía de la seguridad de los productos y servicios que compran o adquieren.

La certificación, que consiste en la evaluación formal de los productos, servicios y procesos por un organismo independiente y acreditado en función de un conjunto de criterios claramente definidos y la expedición de un certificado que atestigüe la conformidad, desempeña un papel importante a la hora de aumentar la confianza y la seguridad en los productos y servicios. Mientras que la evaluación de la seguridad tiene un carácter bastante técnico, la certificación cumple el objetivo de informar y tranquilizar a los compradores y usuarios sobre las propiedades de seguridad de los productos y servicios de TIC que compran o utilizan. Como ya se ha dicho, esto reviste especial importancia en el caso de los nuevos sistemas que hacen amplio uso de las tecnologías digitales y que requieren un alto nivel de seguridad, como los automóviles conectados y automatizados, la sanidad electrónica, los sistemas de control de la automatización industrial (IACS)[14] o las redes inteligentes.

En la actualidad, el paisaje de la certificación de la ciberseguridad de los productos y servicios de TIC en la UE es muy desigual. Existen diversas iniciativas internacionales, como los denominados criterios comunes para la evaluación de la seguridad de la tecnología de la información (ISO 15408), que es una norma internacional para la evaluación de la seguridad informática. Se basa en la evaluación por un tercero y contempla siete niveles de garantía de la evaluación. Los criterios comunes y la metodología común para la evaluación de la seguridad de la tecnología de la información (CEM) asociada constituyen la base técnica de un acuerdo internacional, el Acuerdo de reconocimiento de los criterios comunes (CCRA), que garantiza que los certificados de criterios comunes sean reconocidos por todos sus signatarios. No obstante, en la versión actual del CCRA solo gozan de reconocimiento mutuo

[13] El «plan director» se aplicará a los incidentes de ciberseguridad que causen perturbaciones mayores de las que un Estado miembro puede abordar por sí solo o que afecten a dos o más Estados miembros con un impacto de tanta importancia y alcance o tanta significación política que exige una oportuna coordinación de medidas y una respuesta a nivel político de la Unión.

[14] La DG JRC ha publicado un informe que propone un conjunto inicial de requisitos comunes europeos y directrices generales relativos a la certificación de la ciberseguridad de los componentes de IACS. Disponible en: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

las evaluaciones hasta el nivel 2. Además, solo trece Estados miembros han firmado el Acuerdo.

Las autoridades de certificación de doce Estados miembros han celebrado un acuerdo de reconocimiento mutuo relativo a los certificados expedidos de conformidad con el Acuerdo sobre la base de los criterios comunes[15]. Por otra parte, existen actualmente o se están estableciendo en los Estados miembros una serie de iniciativas de certificación de las TIC. Estas iniciativas, aunque sean importantes, conllevan el riesgo de fragmentar el mercado y provocar problemas de interoperabilidad. En consecuencia, una empresa puede tener que someterse a varios procedimientos de certificación en distintos Estados miembros para poder ofrecer su producto en múltiples mercados. Así, un fabricante de contadores inteligentes que desee vender sus productos en tres Estados miembros, por ejemplo Alemania, Francia y el Reino Unido, tiene que ajustarse actualmente a tres regímenes de certificación diferentes. Se trata del *Commercial Product Assurance* (CPA) en el Reino Unido, la *Certification de Sécurité de Premier Niveau* (CSPN) en Francia y un perfil de protección específico basado en los criterios comunes en Alemania.

Esta situación propicia un incremento de los costes y constituye una carga administrativa considerable para las empresas que operan en varios Estados miembros. Aun cuando el coste de la certificación puede variar considerablemente dependiendo del producto o servicio de que se trate, el nivel de garantía de la evaluación requerido y/u otros componentes, en términos generales suele resultar bastante elevado para las empresas. El certificado *Smart Meter Gateway* del BSI, por ejemplo, tiene un coste superior al millón de euros (nivel más elevado de ensayo y garantía, afecta no solo a un producto, sino a toda la infraestructura que lo rodea). El coste de la certificación de contadores inteligentes en el Reino Unido asciende a casi 150 000 EUR. En Francia, el coste es similar al del Reino Unido, unos 150 000 EUR o más.

Las principales partes interesadas tanto públicas como privadas reconocieron que, en ausencia de un régimen de certificación de la ciberseguridad a escala de la UE, en muchos casos las empresas han de certificarse individualmente en cada Estado miembro, lo que conduce a la fragmentación del mercado. Lo que es más importante, en ausencia de legislación de armonización de la UE para los productos y servicios de TIC, las diferencias en las normas y prácticas de certificación de la ciberseguridad en los Estados miembros pueden crear en la práctica 28 mercados de la seguridad diferentes en la UE, cada uno de ellos con sus propios requisitos técnicos, métodos de ensayo y procedimientos de certificación de la ciberseguridad. Estos enfoques divergentes a nivel nacional pueden provocar, si no se toman medidas adecuadas a nivel de la UE, un importante retraso en la consecución del mercado único digital, ralentizando o anulando los efectos positivos asociados en términos de crecimiento y empleo.

Sobre la base de lo anterior, en el Reglamento propuesto se establece un marco europeo de certificación de la ciberseguridad (el «**Marco**») para los productos y servicios de TIC y se especifican las funciones y tareas esenciales de ENISA en el ámbito de la certificación de la ciberseguridad. La presente propuesta establece un marco general de normas que regulan los regímenes europeos de certificación de la ciberseguridad. La propuesta no introduce

[15] El Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS) incluye a doce Estados miembros más Noruega y ha desarrollado varios perfiles de protección para un número limitado de productos, como la firma digital, el tacógrafo digital y las tarjetas inteligentes. Los participantes trabajan conjuntamente para coordinar la normalización de los perfiles de protección de los criterios comunes, así como el desarrollo de perfiles de protección. Los Estados miembros suelen exigir la certificación SOG-IS en las licitaciones públicas nacionales.

directamente regímenes de certificación operativos, sino que crea un sistema (marco) para el establecimiento de regímenes específicos para productos/servicios de TIC concretos (en lo sucesivo, «regímenes europeos de certificación de la ciberseguridad»). La creación de regímenes europeos de certificación de la ciberseguridad de conformidad con el Marco permitirá que los certificados expedidos con arreglo a dichos regímenes obtengan validez y reconocimiento en todos los Estados miembros y se combata la fragmentación actual del mercado.

El objetivo general de un régimen europeo de certificación de la ciberseguridad es dejar constancia de que los productos y servicios de TIC certificados con arreglo a dicho régimen cumplen unos requisitos de ciberseguridad especificados. Entre ellos figurarían, por ejemplo, su capacidad para proteger los datos (conservados, transmitidos o procesados de la manera que sea) del almacenamiento, tratamiento, acceso, divulgación, destrucción, pérdida o alteración accidentales o no autorizados. Los regímenes de certificación de la ciberseguridad de la UE harían uso de normas existentes en relación con los requisitos técnicos y procedimientos de evaluación que los productos deben cumplir, pero no desarrollarían las normas técnicas en sí[16]. Por ejemplo, una certificación a escala de la UE de productos tales como las tarjetas inteligentes, que actualmente se someten a ensayo en función de normas internacionales de criterios comunes en el marco del sistema multilateral (descrito anteriormente) SOG-IS, significaría que el régimen tendría validez en toda la UE.

Además de indicar un conjunto específico de objetivos de seguridad que deben tenerse en cuenta al diseñar un régimen concreto de certificación de la ciberseguridad de la UE, la propuesta establece el contenido mínimo de este tipo de regímenes. Los regímenes tendrán que definir, entre otras cosas, una serie de elementos específicos que determinan el alcance y objeto de la certificación de ciberseguridad. Esto incluye la indicación de las categorías de productos y servicios cubiertos, la especificación detallada de los requisitos de ciberseguridad (por ejemplo, remitiéndose a las normas o especificaciones técnicas pertinentes), los métodos y criterios específicos de evaluación y el nivel de garantía que se proponen asegurar (a saber, básico, sustancial o elevado).

Los regímenes europeos de certificación de la ciberseguridad serán preparados por ENISA con la asistencia, asesoramiento y estrecha cooperación del Grupo Europeo de Certificación de la Ciberseguridad (véase más adelante), y adoptados por la Comisión mediante actos de ejecución. Cuando se detecte la necesidad de un régimen de certificación de la ciberseguridad, la Comisión solicitará a ENISA que prepare un régimen para determinados productos o servicios de TIC. ENISA trabajará al respecto en estrecha colaboración con las autoridades nacionales de supervisión de la certificación representadas en el Grupo. Los Estados miembros y el Grupo podrán proponer a la Comisión que solicite a ENISA la preparación de un régimen particular.

La certificación puede resultar un proceso muy costoso, que podría traducirse en un alza de los precios para los clientes y los consumidores. La necesidad de certificar puede variar también considerablemente en función del contexto específico de uso de los productos y servicios y de la rapidez del cambio tecnológico. El recurso a la certificación europea de la ciberseguridad debe, por tanto, seguir siendo voluntario, a menos que se disponga otra cosa en la legislación de la Unión que establezca los requisitos de seguridad de productos y servicios de TIC.

[16] En el caso de las normas europeas, esto lo efectúan las organizaciones europeas de normalización y lo refrenda la Comisión Europea con la publicación en el *Diario Oficial* (véase el Reglamento 1025/2012).

Con el fin de garantizar la armonización y evitar la fragmentación, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad dejarán de aplicarse a partir de la fecha establecida en el acto de ejecución por el que se adopte este régimen. Además, los Estados miembros deberían abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad existente.

Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o los proveedores de servicios de TIC tendrán la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deberían ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación revocarán la acreditación de un organismo de evaluación de la conformidad cuando no se cumplan, o hayan dejado de cumplirse, las condiciones de la acreditación, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

Con arreglo a la propuesta, las tareas de seguimiento, supervisión y ejecución recaen en los Estados miembros. Los Estados miembros deberán contar con una autoridad de supervisión de la certificación. Esta autoridad estará encargada de supervisar que los organismos de evaluación de la conformidad, así como los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, se ajustan a los requisitos del presente Reglamento y de los pertinentes regímenes europeos de certificación de la ciberseguridad. Las autoridades nacionales de supervisión de la certificación serán competentes para tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio. En la medida que proceda, investigarán el objeto de la reclamación e informarán en un plazo razonable al reclamante sobre el curso y el resultado de la investigación. Además, cooperarán con otras autoridades de supervisión de la certificación y autoridades públicas, por ejemplo mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o a determinados regímenes europeos de certificación de la ciberseguridad.

Por último, la propuesta establece el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»), constituido por las autoridades nacionales de supervisión de la certificación de todos los Estados miembros. La principal tarea del Grupo es asesorar a la Comisión sobre las cuestiones relativas a la política de certificación de la ciberseguridad y trabajar con ENISA en la elaboración de proyectos de regímenes europeos de certificación de la ciberseguridad. ENISA asistirá a la Comisión a encargarse de la secretaría del Grupo y conservará un inventario público actualizado de los regímenes aprobados en virtud del marco europeo de certificación de la ciberseguridad. ENISA también mantendrá contactos con los organismos de normalización a fin de garantizar la adecuación de las normas utilizadas en regímenes autorizados y detectar ámbitos que precisen de normas de ciberseguridad.

El marco europeo de certificación de la ciberseguridad (en lo sucesivo, «el Marco») aportará diversos beneficios a los ciudadanos y las empresas. En particular:

- La creación de sistemas de certificación de la ciberseguridad a escala de la UE para determinados productos o servicios proporcionará a las empresas una «ventanilla única» para la certificación de la ciberseguridad en la UE. Las empresas estarán en

condiciones de certificar su producto una sola vez y obtener un certificado válido en todos los Estados miembros. No estarán obligadas a volver a certificar sus productos ante diferentes organismos nacionales de certificación. De este modo disminuirán significativamente los costes para las empresas, se facilitarán las operaciones transfronterizas y, en última instancia, se reducirá y evitará la fragmentación del mercado interior de los productos de que se trate.

- El Marco establece la primacía de los regímenes europeos de certificación de la ciberseguridad sobre los nacionales. Por ello, la adopción de un régimen europeo de certificación de la ciberseguridad sustituirá a todos los regímenes nacionales paralelos existentes para los mismos productos o servicios de TIC a un determinado nivel de garantía. Esto aportará más claridad, reduciendo la actual proliferación de regímenes nacionales de certificación de la ciberseguridad que se solapan y posiblemente se contradicen.
- La propuesta sostiene y complementa la aplicación de la Directiva SRI, proporcionando a las empresas sometidas a ella una herramienta muy útil para demostrar el cumplimiento de los requisitos de la SRI en el conjunto de la Unión. Al desarrollar nuevos regímenes de certificación de la ciberseguridad, la Comisión y ENISA prestarán especial atención a la necesidad de garantizar que los requisitos de SRI se vean reflejados en dichos regímenes.
- La propuesta respaldará y facilitará el desarrollo de una política europea de ciberseguridad, armonizando las condiciones y los requisitos sustantivos para la certificación de la ciberseguridad de los productos y servicios de TIC en la UE. Los regímenes europeos de certificación de la ciberseguridad harán referencia a normas o criterios comunes de evaluación y metodologías de ensayo. De este modo, se contribuirá de manera significativa, aunque indirecta, a la asimilación de soluciones de seguridad comunes en la UE y, por ende, a la eliminación de obstáculos al mercado interior.
- El Marco está concebido con vistas a garantizar la flexibilidad necesaria para los regímenes de certificación de la ciberseguridad. En función de las necesidades específicas en materia de ciberseguridad, un producto o servicio podrá ser certificado en función de niveles de seguridad más o menos elevados. Los regímenes europeos de certificación de la ciberseguridad se diseñarán teniendo en mente esta flexibilidad y, por lo tanto, aportarán distintos niveles de garantía (a saber, básico, sustancial o elevado) con el fin de que puedan usarse con fines distintos o en contextos diferentes.
- En virtud de todos los elementos mencionados, la certificación de la ciberseguridad resultará más atractiva para las empresas como medio eficaz de comunicar el nivel de garantía de la ciberseguridad de los productos o servicios de TIC. En la medida en que la certificación de la ciberseguridad resulte más barata, eficaz y comercialmente atractiva, las empresas tendrán un mayor incentivo para certificar sus productos frente a los riesgos en materia de ciberseguridad, contribuyendo así a la difusión de las mejores prácticas de ciberseguridad en el diseño de productos y servicios de TIC (ciberseguridad a través del diseño).

- **Coherencia con las disposiciones existentes en la misma política sectorial**

En virtud de la Directiva SRI, los operadores de los sectores que son vitales para nuestra economía y sociedad, como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad y la infraestructura digital, así como los proveedores de

servicios digitales (por ejemplo, motores de búsqueda, servicios de computación en la nube y mercados en línea) están obligados a tomar las medidas necesarias para gestionar adecuadamente los riesgos para la seguridad. Las nuevas normas de la presente propuesta complementan las disposiciones de la Directiva SRI y garantizan la coherencia con ellas para fortalecer la ciberresiliencia de la UE mediante la mejora de las capacidades, la cooperación, la gestión de riesgos y la sensibilización.

Por otra parte, las normas sobre certificación de la ciberseguridad ponen una herramienta esencial en manos de las empresas sujetas a la Directiva SRI, dado que podrán certificar sus productos y servicios de TIC frente a los riesgos de ciberseguridad sobre la base de regímenes de certificación de la ciberseguridad válidos y reconocidos en todo el territorio de la UE. También serán complementarias de los requisitos de seguridad mencionados en el Reglamento eIDAS[17] y la Directiva sobre equipos radioeléctricos[18].

- **Coherencia con otras políticas de la Unión**

El Reglamento (UE) 2016/679 (Reglamento general de protección de datos o «**RGPD**»)[19] contiene disposiciones para establecer mecanismos de certificación y sellos y marcas de protección de datos a fin de demostrar la conformidad con el Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del RGPD, incluso cuando dichas operaciones se encuentran integradas en productos y servicios.

El Reglamento propuesto garantizará la compatibilidad con el Reglamento (CE) n.º 765/2008 sobre los requisitos de acreditación y de vigilancia del mercado[20] haciendo referencia a las normas de dicho marco sobre los organismos nacionales de acreditación y de evaluación de la conformidad. En lo que respecta a las autoridades de supervisión, el Reglamento propuesto exigirá que los Estados miembros designen autoridades nacionales de supervisión de la certificación responsables de la supervisión, el seguimiento y la ejecución de las normas. Estos organismos serán independientes de los organismos de evaluación de la conformidad prescritos en el Reglamento (CE) n.º 765/2008.

---

17 Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

18 Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE.

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

20 Reglamento (CE) n.º 765/2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- **Base jurídica**

La base jurídica de la acción de la UE es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que se refiere a la aproximación de las legislaciones de los Estados miembros a fin de alcanzar los objetivos del artículo 26 del TFUE, a saber, el correcto funcionamiento del mercado interior.

La base jurídica relativa al mercado interior para la creación de ENISA fue respaldada por el Tribunal de Justicia (asunto C-217/04 *Reino Unido contra Parlamento Europeo y Consejo*) y confirmada nuevamente por el Reglamento de 2013 que estableció el mandato actual de la Agencia. Además, las actividades que reflejasen los objetivos de aumentar la cooperación y la coordinación entre los Estados miembros y añadiesen capacidades a nivel de la UE para complementar la acción de los Estados miembros entrarían en la categoría de «cooperación operativa». La Directiva SRI (cuya base jurídica es el artículo 114 del TFUE) la señala específicamente como objetivo que debe perseguirse en el marco de la red de CSIRT, pues «ENISA se hará cargo de la secretaría y apoyará activamente la cooperación» (artículo 12, apartado 2). En particular, el artículo 12, apartado 3, letra f), indica también la identificación de otras formas de cooperación operativa como tarea de la red de CSIRT, en particular en relación con: i) categorías de riesgos e incidentes, ii) alertas tempranas, iii) asistencia mutua, y iv) principios y modalidades de coordinación, cuando los Estados miembros respondan a incidentes y riesgos transfronterizos.

- La actual fragmentación de los regímenes de certificación de productos y servicios de TIC es también consecuencia de la falta de un marco común, eficaz y jurídicamente vinculante, aplicable a los Estados miembros. Esto dificulta la creación de un mercado interior de productos y servicios de TIC y obstaculiza la competitividad de la industria europea en el sector. La presente propuesta tiene por objeto combatir la fragmentación existente y los obstáculos relacionados con el mercado interior ofreciendo un marco común para el establecimiento de regímenes de certificación de la ciberseguridad válidos en toda la UE.

Subsidiariedad (en el caso de competencia no exclusiva)

El principio de subsidiariedad exige evaluar la necesidad y el valor añadido de la acción de la UE. El respeto de la subsidiariedad en este ámbito se reconoció ya en el momento de adoptar el actual Reglamento de ENISA[21].

La ciberseguridad es una cuestión de interés común de la Unión. Las interdependencias entre las redes y los sistemas de información son tales que muy a menudo los diferentes agentes (públicos y privados, incluidos los ciudadanos) no pueden hacer frente por sí solos a las amenazas y gestionar los riesgos y las posibles repercusiones de los ciberincidentes. Por una parte, las interdependencias entre los Estados miembros, en particular en lo que se refiere a la explotación de las infraestructuras críticas (energía, transporte o agua, por citar solo algunas) hacen que la intervención pública a nivel europeo resulte no solo beneficiosa, sino también necesaria. Por otra, la intervención de la UE puede aportar un efecto «de contagio» positivo

[21] Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004.

gracias al intercambio de buenas prácticas entre los Estados miembros, lo que puede dar lugar a una mejora de la ciberseguridad de la Unión.

En resumen, en el contexto actual y teniendo en cuenta las perspectivas de futuro, parece que si se quiere **incrementar la ciberresiliencia colectiva** de la Unión, las **actuaciones individuales de sus Estados miembros y un enfoque fragmentado en materia de ciberseguridad** no serán suficientes.

La intervención de la UE también se considera necesaria para hacer frente a la fragmentación de los actuales regímenes de certificación de la ciberseguridad. Permitiría que los fabricantes se beneficiasen plenamente de un mercado interior, con ahorros significativos en relación con los costes de ensayo y rediseño. Aun cuando el actual Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS) ha logrado, por ejemplo, resultados considerables en este sentido, también ha acusado limitaciones importantes que merman su idoneidad para ofrecer soluciones sostenibles a largo plazo que permitan aprovechar todas las posibilidades del mercado interior.

El valor añadido de la actuación a nivel de la UE, en particular para reforzar la cooperación entre los Estados miembros, pero también entre las comunidades de la seguridad de las redes y de la información, fue reconocido por las Conclusiones del Consejo de 2016[22] y también se desprende claramente de la evaluación de ENISA.

- **Proporcionalidad**

La medida propuesta no excede de lo necesario para alcanzar sus objetivos. Además, el ámbito de la intervención de la UE no impide ulteriores medidas nacionales en el campo de la seguridad nacional. Por lo tanto, la acción de la UE está justificada en cuanto a la subsidiariedad y la proporcionalidad.

- **Elección del instrumento**

La presente propuesta revisa el Reglamento (UE) n.º 526/2013, que establece el mandato y las tareas actuales de ENISA. Además, habida cuenta del importante papel de ENISA en la creación y gestión de un marco de certificación de la ciberseguridad de la UE, conviene establecer el nuevo mandato de ENISA y el citado marco en un único instrumento jurídico, utilizando como instrumento un Reglamento.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

Evaluaciones *ex post* / control de calidad de la legislación existente

La Comisión, de acuerdo con la hoja de ruta de la evaluación[23], evaluó la **pertinencia, repercusión, eficacia, eficiencia, coherencia y valor añadido** de la Agencia en lo que se refiere a su rendimiento, gobernanza, estructura organizativa interna y prácticas de trabajo durante el período 2013-2016. Los resultados principales pueden resumirse del siguiente

[22] Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

modo (para más información, véase el documento de trabajo de los servicios sobre el tema, que acompaña a la evaluación de impacto).

- **Pertinencia:** En un contexto de avances tecnológicos y amenazas cambiantes, y teniendo en cuenta la significativa necesidad de reforzar la ciberseguridad en la UE, los objetivos de ENISA se han demostrado pertinentes. De hecho, los Estados miembros y los organismos de la UE confían en sus sustanciales conocimientos en materia de ciberseguridad. Además, deben desarrollarse en los Estados miembros capacidades que permitan comprender y responder mejor a las amenazas, y es precisa una cooperación de las partes interesadas de todos los ámbitos temáticos e instituciones. La ciberseguridad sigue siendo una prioridad política clave de la UE a la que se espera responda ENISA; sin embargo, el diseño de ENISA como agencia de la UE con un mandato de duración determinada: i) no permite una planificación a largo plazo y un apoyo sostenible a los Estados miembros y las instituciones de la UE, ii) puede dar lugar a un vacío legal en la medida en que las disposiciones de la Directiva SRI encomiendan a ENISA tareas de carácter permanente[24], iii) carece de coherencia con una visión que vincule a ENISA con un ecosistema de ciberseguridad de la UE reforzado.
- **Eficacia**: ENISA alcanzó en general sus objetivos y desempeñó sus cometidos. Contribuyó al incremento de la seguridad de las redes y de la información en Europa por medio de sus actividades principales (creación de capacidades, asistencia técnica, creación de comunidades y apoyo a las políticas). Sin embargo, mostró que había margen de mejora en relación con cada una de ellas. La evaluación llegó a la conclusión de que ENISA ha creado efectivamente unas relaciones sólidas y de confianza con algunas de sus partes interesadas, especialmente con los Estados miembros y la comunidad de CSIRT. Las intervenciones en materia de creación de capacidades se consideraron eficaces, en particular en los Estados miembros que cuentan con menos recursos. El estímulo de una amplia cooperación ha sido uno de los aspectos más destacados, coincidiendo las partes interesadas en el papel positivo que desempeña ENISA para acercar a las personas. Sin embargo, ENISA encontró dificultades para lograr un impacto notable en el extenso campo de la seguridad de las redes y de la información. Ello se debió también al hecho de que dispuso de unos recursos humanos y financieros bastante limitados para cumplir un mandato muy amplio. La evaluación también llegó a la conclusión de que ENISA alcanzó parcialmente el objetivo de proporcionar asesoramiento, dados los problemas para contratar expertos (véase también la sección sobre eficiencia).
- **Eficiencia**: A pesar de su reducido presupuesto (entre los más bajos de las agencias de la UE), la Agencia ha sido capaz de contribuir a alcanzar objetivos concretos, demostrando una eficiencia global en el uso de sus recursos. La evaluación concluyó que los procesos eran por regla general eficientes y que la clara delimitación de responsabilidades dentro de la organización propiciaba una buena ejecución del trabajo. Uno de los principales retos para la eficiencia de la Agencia guarda relación con las dificultades de ENISA para contratar y retener a expertos altamente cualificados. Las conclusiones muestran que esto se puede explicar por una combinación de factores, entre los que figuran las dificultades de carácter general del sector público para competir con el privado en la contratación de expertos altamente

[24] Referencia a los artículos 7, 9, 11, 12 y 19 de la Directiva sobre Seguridad de las Redes y los Sistemas de Información (Directiva SRI).

especializados, el tipo de contrato (temporal) que la Agencia podría ofrecer básicamente y el escaso atractivo de la ubicación de ENISA en lo que se refiere, por ejemplo, a las dificultades de los cónyuges para encontrar trabajo. La doble localización en Atenas y Heraklion exigió esfuerzos adicionales de coordinación y generó costes suplementarios, pero el traslado a Atenas en 2013 del departamento de operaciones esenciales reforzó la eficacia operativa de la Agencia.

- **Coherencia**: Las actividades de ENISA han sido coherentes por regla general con las políticas y actividades de las partes interesadas, a escala nacional y de la UE, pero es necesario un enfoque más coordinado a nivel de la UE en materia de ciberseguridad . No se ha aprovechado plenamente el potencial para la cooperación entre ENISA y otros organismos de la UE. La evolución del panorama jurídico y político de la UE hace que el vigente mandato resulte menos coherente en la actualidad.

- **Valor añadido de la UE**: El valor añadido de ENISA radica principalmente en la capacidad de la Agencia para mejorar la cooperación, principalmente entre los Estados miembros, pero también con las comunidades de la seguridad de las redes y de la información relacionadas. No existe ningún otro agente a nivel de la UE que facilite la cooperación de una variedad análoga de partes interesadas en la seguridad de las redes y de la información. El valor añadido aportado por la Agencia osciló en función de las diferentes necesidades y recursos de sus partes interesadas (por ejemplo, Estados miembros grandes o pequeños; Estados miembros e industria) y de la necesidad de que la Agencia priorizase sus actividades con arreglo al programa de trabajo. La evaluación llegó a la conclusión de que una eventual clausura de ENISA representaría la pérdida de una oportunidad para todos los Estados miembros. No será posible garantizar el mismo grado de creación de comunidades y cooperación en los Estados miembros en el ámbito de la ciberseguridad. Sin una agencia de la UE más centralizada, la fragmentación aumentaría y la cooperación bilateral o regional intentaría colmar el vacío dejado por ENISA.

En lo que se refiere concretamente al rendimiento pasado y al futuro de ENISA, las principales tendencias que se desprenden de la consulta de 2017 son las siguientes[25]:

- El rendimiento global de ENISA durante el período de 2013 a 2016 fue evaluado positivamente en la mayoría de las respuestas (74 %). También fue mayoritaria la opinión de que ENISA estaba alcanzando sus diferentes objetivos (al menos un 63 % para cada uno de los objetivos). Los servicios y productos de ENISA son utilizados de forma regular (mensualmente o con mayor frecuencia) por casi la mitad de quienes respondieron (46 %) y apreciados por el hecho de proceder de un organismo a nivel de la UE (83 %) y por su calidad (62 %).

- En las respuestas se mencionan diversas lagunas y retos para el futuro de la ciberseguridad en la UE, siendo los cinco principales (en una lista de 16): la

[25] Respondieron a la consulta 90 partes interesadas procedentes de 19 Estados miembros (88 respuestas y 2 documentos de posición), incluidas las autoridades nacionales de 15 Estados miembros, incluidos Francia, Italia, Irlanda y Grecia y 8 organizaciones representativas de un gran número de organizaciones europeas, como por ejemplo la Federación Bancaria Europea, Europa Digital (en representación de la industria de la tecnología digital en Europa) o la Asociación de Operadores Europeos de Redes de Telecomunicación (ETNO). La consulta pública sobre ENISA se complementó con otras fuentes diversas, entre ellas: i) entrevistas en profundidad con unos 50 agentes clave del colectivo de la ciberseguridad, ii) una encuesta a la red de CSIRT, iii) una encuesta al Consejo de Administración, al Comité Ejecutivo y al Grupo Permanente de Partes Interesadas de ENISA.

cooperación entre los Estados miembros; la capacidad para prevenir, detectar y solucionar los ciberataques a gran escala; la cooperación entre los Estados miembros en las cuestiones relacionadas con la ciberseguridad; la cooperación y el intercambio de información entre las distintas partes interesadas, incluida la cooperación entre los sectores público y privado; la protección de las infraestructuras críticas frente a ciberataques.

- Una gran mayoría (88 %) de las respuestas consideraba que los actuales instrumentos y mecanismos disponibles a nivel de la UE son insuficientes o adecuados solo parcialmente para abordar estos problemas. Una gran mayoría de las respuestas (98 %) indicó que un organismo de la UE debía dar respuesta a estas necesidades y, entre ellos, el 99 % consideraba que ENISA era la organización adecuada para ello.

Consultas con las partes interesadas

- La Comisión organizó una consulta pública para la revisión de ENISA, abierta entre el 12 de abril y el 5 de julio de 2016, y recibió 421 respuestas[26]. Según los resultados, el 67,5 % de las respuestas expresaron la opinión de que ENISA podría desempeñar cierto papel en el establecimiento de un marco armonizado para la certificación de la seguridad de los productos y servicios de TI.

Los resultados de la consulta de 2016 sobre la APP contractual de ciberseguridad[27], en la sección relativa a la certificación, muestran que:

- El 50,4 % (121 de 240) desconoce si los regímenes nacionales de certificación están reconocidos mutuamente en los Estados miembros de la UE. El 25,8 % (62 de 240) responde «no», mientras que el 23,8 % (57 de 240) responde «sí».
- El 37,9 % de las respuestas (91 de 240) considera que los actuales regímenes de certificación no atienden las necesidades de la industria europea. Por otra parte, en 17,5 % (42 de 240), principalmente empresas internacionales que operan en el mercado europeo, opina lo contrario.
- El 49,6 % (119 de 240) de las respuestas afirma que no es fácil demostrar la equivalencia entre normas, regímenes de certificación y etiquetas. El 37,9 % (91 de 240) responde «no lo sé», mientras que solo el 12,5 % (30 de 240) responde «sí».

Obtención y uso de asesoramiento especializado

La Comisión se basó en el siguiente asesoramiento externo:

- *Study on the Evaluation of ENISA* (Estudio de evaluación de ENISA) (Ramboll/Carsa 2017; SMART n.º 2016/0077),
- *Study on ICT Security Certification and labelling – Evidence gathering and impact assessment* (Estudio sobre certificación y el etiquetado de seguridad de las TIC —

[26] A saber, 162 contribuciones de ciudadanos, 33 de organizaciones de consumidores y de la sociedad civil, 186 del sector y 40 de las administraciones públicas, incluidas las autoridades competentes encargadas de la aplicación de la Directiva sobre privacidad y comunicaciones electrónicas.

[27] Respondieron a la sección relativa a la certificación 240 representantes de las administraciones públicas nacionales, las grandes empresas, las pymes, las microempresas y los organismos de investigación.

Recogida de pruebas y evaluación de impacto) (PriceWaterhouseCoopers 2017; SMART n.º 2016/0029).

Evaluación de impacto

El informe de evaluación de impacto sobre esta iniciativa señaló los siguientes problemas principales que deben abordarse:

- fragmentación de las políticas y enfoques en materia de ciberseguridad en los distintos Estados miembros;
- dispersión de los recursos y fragmentación de los enfoques en materia de ciberseguridad en las instituciones, órganos y organismos de la UE; e
- insuficiencia de los conocimientos e información de los ciudadanos y las empresas, junto con la creciente aparición de múltiples regímenes de certificación nacionales y sectoriales.

El informe evaluó las siguientes posibles opciones en relación con el mandato de ENISA:

- mantenimiento del *statu quo*, es decir, mandato ampliado pero todavía limitado en el tiempo (opción de referencia);
- expiración del mandato actual de ENISA sin renovación y cierre de ENISA (ausencia de intervención);
- una «reforma de ENISA»; y
- una agencia de ciberseguridad de la UE con plena capacidad operativa.

El informe evaluó las siguientes posibles opciones en relación con la certificación de la ciberseguridad:

- ausencia de intervención (opción de referencia);
- medidas no legislativas (Derecho indicativo);
- un acto legislativo de la Unión con el fin de crear un régimen obligatorio para todos los Estados miembros basado en el sistema SOG-IS; y
- un marco general de certificación de la ciberseguridad de las TIC en la UE.

El análisis llevó a la conclusión de que la opción preferida es una «reforma de ENISA», combinada con un marco general de la UE para la certificación de la ciberseguridad de las TIC.

La opción preferida ha sido considerada la más eficaz para que la UE alcance los objetivos de: aumentar las capacidades de ciberseguridad, preparación, cooperación, sensibilización, transparencia y evitación de la fragmentación del mercado. También la más coherente con las prioridades políticas de la Estrategia de Ciberseguridad de la UE y sus demás políticas relacionadas (por ejemplo, la Directiva SRI) y la Estrategia para el Mercado Único Digital. Además, el proceso de consulta puso de manifiesto que la opción preferida cuenta con el apoyo de la mayoría de las partes interesadas. El análisis efectuado en la evaluación de impacto mostró asimismo que la opción preferida permitiría alcanzar los objetivos mediante un empleo razonable de los recursos.

El Comité de Control Reglamentario de la Comisión emitió inicialmente un dictamen negativo el 24 de julio, y posteriormente un dictamen favorable tras una nueva presentación el 25 de agosto de 2017. El informe de evaluación de impacto modificado incorporaba nuevos

justificativos, las conclusiones finales de la evaluación de ENISA y explicaciones adicionales sobre las opciones políticas y su impacto. El anexo 1 del informe final sobre la evaluación de impacto resume cómo se había respondido a las observaciones del Comité en el segundo dictamen. En particular, se actualizó el informe para incorporar con mayor detalle el contexto de ciberseguridad de la UE, incluidas las medidas que figuran en la Comunicación conjunta «Resiliencia, disuasión y defensa: Reforzar la ciberseguridad de la UE» [JOIN(2017) 450] y tienen una especial relevancia para ENISA: el plan director de ciberseguridad de la UE y el Centro Europeo de Investigación y Competencias sobre Ciberseguridad, al que la Agencia sometería sus recomendaciones sobre las necesidades de la UE en materia de investigación.

El informe explica cómo la reforma de la Agencia, incluidas las nuevas funciones, las mejores condiciones de empleo y la cooperación estructural con los órganos de la UE en este ámbito, podría mejorar su atractivo como empleador y ayudar a afrontar los problemas relacionados con la contratación de expertos. El anexo 6 del informe presenta también una estimación revisada de los costes asociados a las opciones políticas de ENISA. En relación con el tema de la certificación, se ha revisado el informe con el fin de proporcionar una explicación más detallada, incluida una presentación gráfica, de la opción preferida, y de ofrecer estimaciones sobre los costes para los Estados miembros y la Comisión en relación con el nuevo marco de certificación. También se ha justificado la elección de ENISA como agente clave en el marco sobre la base de su experiencia en este ámbito y el hecho de ser la única agencia de ciberseguridad a nivel de la UE. Por último, se han revisado las secciones sobre certificación para aclarar los aspectos relacionados con la diferencia con el actual sistema SOG-IS y los beneficios asociados a las diferentes opciones y para explicar el hecho de que el tipo de producto y servicio de TIC cubierto por un régimen europeo de certificación se defina en el propio régimen aprobado.

Adecuación regulatoria y simplificación

No procede

Impacto en los derechos fundamentales

La ciberseguridad desempeña un papel esencial en la protección de los datos personales y la intimidad de las personas físicas de conformidad con lo dispuesto en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE. Cuando se produce un ciberincidente, la intimidad y la protección de nuestros datos personales quedan claramente en entredicho. La ciberseguridad es, pues, condición necesaria para el respeto de la intimidad y la confidencialidad de nuestros datos personales. Desde esta perspectiva, con el objetivo de reforzar la ciberseguridad en Europa, la propuesta constituye un importante complemento de la legislación vigente que protege el derecho fundamental al respeto de la intimidad y de los datos personales. La ciberseguridad es esencial asimismo para proteger la confidencialidad de nuestras comunicaciones electrónicas y, por tanto, para ejercer la libertad de expresión y de información y otros derechos afines, tales como la libertad de pensamiento, conciencia y religión.

4. REPERCUSIONES PRESUPUESTARIAS

Véase la ficha financiera

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

La Comisión supervisará la aplicación del Reglamento y presentará cada cinco años un informe sobre su evaluación al Parlamento Europeo y al Consejo, así como al Comité Económico y Social Europeo. Estos informes serán públicos y analizarán la aplicación y el cumplimiento efectivos del presente Reglamento.

- **Explicación detallada de las disposiciones específicas de la propuesta**

El título I del Reglamento contiene las disposiciones generales: el objeto (artículo 1), las definiciones (artículo 2), incluidas las referencias a las definiciones pertinentes de otros instrumentos de la UE, como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI), el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93, y el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, sobre la normalización europea.

El título II del Reglamento contiene las disposiciones clave relacionadas con ENISA, la Agencia de Ciberseguridad de la UE.

El capítulo I de este título describe el mandato (artículo 3), los objetivos (artículo 4) y las funciones de la Agencia (artículos 5 a 11).

El capítulo II describe la organización de ENISA y contiene disposiciones fundamentales sobre su estructura (artículo 12). Aborda la composición, las normas de votación y las funciones del Consejo de Administración (sección 1, artículos 13 a 17), del Comité Ejecutivo (sección 2, artículo 18) y del director ejecutivo (Sección 3, artículo 19). También incluye disposiciones sobre la composición y funciones del Grupo Permanente de Partes Interesadas (Sección 4, artículo 20). Por último, la sección 5 del capítulo detalla las normas operativas de la Agencia, en particular en lo que respecta a la programación de sus operaciones, conflictos de intereses, transparencia, confidencialidad y acceso a los documentos (artículos 21 a 25).

El capítulo III se refiere al establecimiento y la estructura del presupuesto de la Agencia (artículos 26 y 27), así como a las normas que rigen su aplicación (artículos 28 y 29). Incluye, asimismo, disposiciones para facilitar la lucha contra el fraude, la corrupción y otras actividades ilícitas (artículo 30).

El capítulo IV se refiere a la dotación de personal de la Agencia. Incluye disposiciones generales sobre el Estatuto y el Régimen aplicable y las normas sobre privilegios e inmunidades (artículo 31 y 32). Asimismo, se detallan las normas de contratación y nombramiento del director ejecutivo de la Agencia (artículo 33). Por último, incluye las disposiciones que rigen la utilización de expertos nacionales en comisión de servicios u otro personal no contratado por la Agencia (artículo 34).

Finalmente, el capítulo V reúne las disposiciones generales relativas a la Agencia. Indica su estatuto jurídico (artículo 35) e incluye disposiciones que regulan las cuestiones de responsabilidad, régimen lingüístico, protección de los datos personales (artículos 36-38), así como las normas de seguridad sobre la protección de la información clasificada y de la información sensible no clasificada (artículo 40). En él se describen las normas que regulan la cooperación de la Agencia con terceros países y organizaciones internacionales (artículo 39). Por último, contiene disposiciones relativas a la sede de la Agencia y las condiciones

operativas, así como al control administrativo por parte del Defensor del Pueblo (artículos 41 y 42).

El título III del Reglamento establece el marco europeo de certificación de la ciberseguridad (el «**Marco**») para los productos y servicios de TIC como *lex generalis* (artículo 1). Define el objetivo general de los regímenes europeos de certificación de la ciberseguridad, a saber, garantizar que los productos y servicios de TIC cumplan los requisitos de ciberseguridad especificados en lo que respecta a su capacidad para resistir, con un nivel de garantía dado, las acciones que comprometan la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados, o las funciones relacionadas o los servicios (artículo 43). Por otra parte, enumera los objetivos de seguridad que deben proponerse los regímenes europeos de certificación de la ciberseguridad (artículo 45), como por ejemplo la capacidad para proteger los datos del acceso o la revelación, destrucción o alteración accidentales o no autorizados y el contenido (es decir, los elementos) de los regímenes europeos de certificación de la ciberseguridad, por ejemplo la definición detallada de su ámbito de aplicación, los objetivos de seguridad, los criterios de evaluación, etc. (artículo 47).

El título III establece también los principales efectos jurídicos de los regímenes europeos de certificación de la ciberseguridad, a saber, i) la obligación de aplicar el régimen a nivel nacional y el carácter voluntario de la certificación, ii) el hecho de que los regímenes europeos de certificación de la ciberseguridad invaliden los regímenes nacionales relativos a los mismos productos o servicios (artículos 48 y 49).

Este título establece asimismo el procedimiento para la adopción de los regímenes europeos de certificación de la ciberseguridad y las funciones respectivas de la Comisión, ENISA y el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») (artículo 44). Por último, establece las disposiciones relativas a los organismos de evaluación de la conformidad, incluidos sus requisitos, competencias y funciones, las autoridades nacionales de supervisión de la certificación y las sanciones.

Se establece asimismo en este título el Grupo como organismo esencial integrado por representantes de las autoridades nacionales de supervisión de la certificación, cuya función principal es trabajar con ENISA en la preparación de los regímenes europeos de certificación de la ciberseguridad y asesorar a la Comisión sobre cuestiones generales o específicas relativas a la política de certificación de la ciberseguridad.

El título IV del Reglamento contiene las disposiciones finales que describen el ejercicio de la delegación, los requisitos de evaluación, la derogación y sucesión, así como la entrada en vigor.

2017/0225 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité Económico y Social Europeo[28],

Visto el dictamen del Comité de las Regiones[29],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

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

(2) La utilización de las redes y los sistemas de información por los ciudadanos, empresas y administraciones de toda la Unión está ya muy generalizada. La digitalización y la conectividad se convierten en elementos básicos en un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera el despliegue en la UE de millones, si no miles de millones, de dispositivos digitales conectados durante la próxima década. Mientras aumenta el número de dispositivos conectados a internet, la seguridad y la resiliencia no se tienen suficientemente en cuenta desde el diseño, lo que provoca insuficiencias en la ciberseguridad. En este contexto, el uso limitado de la certificación priva a los usuarios individuales y las organizaciones de información suficiente sobre las características de ciberseguridad de los productos y servicios de TIC y socava la confianza en las soluciones digitales.

(3) La intensificación de la digitalización y la conectividad dará lugar a un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resultará más

[28] DO C […] de […], p. […].
[29] DO C […] de […], p. […].

vulnerable a las ciberamenazas y se exacerbarán los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar este riesgo para la sociedad, es preciso adoptar las medidas necesarias para mejorar la ciberseguridad en la UE con vistas a proteger mejor de las ciberamenazas las redes y los sistemas de información, las redes de telecomunicaciones y los productos, servicios y dispositivos digitales utilizados por los ciudadanos, los gobiernos y las empresas, desde las pymes a los operadores de infraestructuras críticas.

(4) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y ciberataques, requieren unas defensas más sólidas. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las respuestas políticas de las autoridades de ciberseguridad y las competencias policiales son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la UE. Esta situación requiere una respuesta y una gestión de crisis efectivas a nivel de la UE, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad europea y la asistencia mutua. En consecuencia, también una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables, y una previsión sistemática de los futuros avances, retos y amenazas, tanto en la Unión como en el mundo, son importantes para los responsables políticos, la industria y los usuarios.

(5) A la luz de los crecientes retos que tiene planteados la Unión en materia de ciberseguridad, es necesario un conjunto completo de medidas que se apoye en actuaciones previas de la Unión y promueva objetivos que se refuercen mutuamente. Entre ellas se incluye la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación y la coordinación en los Estados miembros y las instituciones, órganos y organismos de la UE. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades a nivel de la Unión que podrían complementar la acción de los Estados miembros, en particular en caso de ciberincidentes y crisis transfronterizas a gran escala. Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones de ciberseguridad. Además, debe reforzarse la confianza en el mercado único digital ofreciendo información transparente sobre el nivel de seguridad de los productos y servicios de TIC. Esto puede verse facilitado por una certificación a escala de la UE que aporte requisitos y criterios de evaluación de la ciberseguridad comunes en todos los mercados y sectores nacionales.

(6) En 2004 el Parlamento Europeo y el Consejo adoptaron el Reglamento (CE) n.º 460/2004[30] por el que se creaba ENISA con el objetivo de contribuir a garantizar un nivel efectivo y elevado de seguridad de las redes y de la información dentro de la Unión y a desarrollar una cultura de la seguridad de las redes y de la información en beneficio de ciudadanos, consumidores, empresas y administraciones públicas. En 2008, el Parlamento Europeo y el Consejo adoptaron el Reglamento (CE) n.º 1007/2008[31], que prorrogaba el mandato de la Agencia hasta marzo de 2012. El

[30] Reglamento (CE) n.° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

[31] Reglamento (CE) n.º 1007/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, que modifica el Reglamento (CE) n.º 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, en lo que respecta a su duración (DO L 293 de 31.10.2008, p. 1).

Reglamento (CE) n.º 580/2011[32] prorrogó nuevamente dicho mandato hasta el 13 de septiembre de 2013. En 2013, el Parlamento Europeo y el Consejo adoptaron el Reglamento (UE) n.º 526/2013[33] relativo a ENISA y por el que se derogaba el Reglamento (CE) n.º 460/2004, que prorrogaba el mandato de la Agencia hasta junio de 2020.

(7) La Unión ha adoptado ya medidas importantes para garantizar la ciberseguridad y aumentar la confianza en las tecnologías digitales. En 2013, se adoptó una Estrategia de ciberseguridad de la UE para orientar la respuesta política de la Unión a las amenazas y riesgos relacionados con la ciberseguridad. En su esfuerzo por proteger mejor a los europeos en línea, la Unión adoptó en 2016 el primer acto legislativo en el ámbito de la ciberseguridad, la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en lo sucesivo, «Directiva SRI»). La Directiva SRI instauró requisitos relativos a las capacidades nacionales en el ámbito de la ciberseguridad, estableció los primeros mecanismos para mejorar la cooperación estratégica y operativa entre los Estados miembros e introdujo obligaciones relativas a medidas de seguridad y notificaciones de incidentes en todos los sectores fundamentales para la economía y la sociedad, como la energía, los transportes, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad, las infraestructuras digitales, así como los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea). Se atribuyó un papel clave a ENISA para respaldar la aplicación de esta Directiva. Además, una lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, contribuyendo al objetivo general de conseguir un elevado nivel de ciberseguridad.

(8) Se reconoce que, desde la adopción de la Estrategia de ciberseguridad de la UE de 2013 y la última revisión del mandato de la Agencia, el contexto político general ha cambiado considerablemente, en particular en relación con un contexto mundial más incierto y menos seguro. En este contexto, y en el marco de la nueva política de ciberseguridad de la Unión, es necesario revisar el mandato de ENISA para definir su función en el ecosistema en mutación de la ciberseguridad y garantizar que contribuya eficazmente a configurar la respuesta de la Unión a los desafíos derivados de esta transformación radical del panorama de las amenazas, para lo cual no basta, como reconoció la evaluación de la Agencia, el actual mandato.

(9) La Agencia establecida por el presente Reglamente debe suceder a ENISA, tal como fue establecida por el Reglamento (UE) n.º 526/2013. La Agencia debe llevar a cabo las tareas que le confiere el presente Reglamento y los actos jurídicos de la Unión en el ámbito de la ciberseguridad aportando, entre otras cosas, conocimientos y asesoramiento y actuando como centro de información y conocimientos de la Unión. Debe fomentar el intercambio de mejores prácticas entre los Estados miembros y las partes interesadas del sector privado, sugiriendo políticas a la Comisión Europea y los Estados miembros, actuando como punto de referencia para las iniciativas políticas

[32] Reglamento (UE) n.º 580/2011 del Parlamento Europeo y del Consejo, de 8 de junio de 2011, que modifica el Reglamento (CE) n.º 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, en lo que respecta a su duración (DO L 165 de 24.6.2011, p. 3).

[33] Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004 (DO L 165 de 18.6.2013, p. 41).

sectoriales de la Unión en lo que respecta a la ciberseguridad y fomentando la cooperación operativa entre los Estados miembros, así como entre los Estados miembros y las instituciones, órganos y organismos de la UE.

(10) En el marco de la Decisión 2004/97/CE, Euratom, adoptada en la reunión del Consejo Europeo celebrada el 13 de diciembre de 2003, los representantes de los Estados miembros decidieron que ENISA tendría su sede en una ciudad de Grecia que determinaría el Gobierno griego. El Estado miembro que acoge a la Agencia debe ofrecer las mejores condiciones posibles para un funcionamiento fluido y eficaz de la misma. Para el desempeño correcto y eficaz de sus funciones, para atraer y conservar al personal y para facilitar el establecimiento de contactos con el exterior, es necesario que la Agencia tenga su sede en un lugar adecuado que, entre otras cosas, ofrezca conexiones de transporte adecuadas y servicios para los cónyuges y los hijos que acompañen a su personal. Las disposiciones necesarias deben recogerse en un acuerdo entre la Agencia y el Estado miembro anfitrión, cuya celebración ha de contar con la aprobación del Consejo de Administración de la Agencia.

(11) En vista de los crecientes retos en materia de ciberseguridad a que se enfrenta la Unión, deben incrementarse los recursos financieros y humanos asignados a la Agencia, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crítica en el ecosistema de organizaciones que defienden el ecosistema digital europeo.

(12) La Agencia debe desarrollar y mantener un elevado nivel de conocimientos técnicos y actuar como punto de referencia que genere confianza en el mercado único en virtud de su independencia, la calidad del asesoramiento prestado y la información difundida, la transparencia de sus procedimientos y métodos de funcionamiento y su diligencia en el desempeño de sus tareas. La Agencia debe contribuir proactivamente a los esfuerzos nacionales y de la Unión y desempeñar sus funciones cooperando plenamente con las instituciones, órganos y organismos de la Unión y los Estados miembros. Además, la Agencia debe apoyarse en las aportaciones del sector privado y en la cooperación con el mismo, así como con otras partes interesadas pertinentes. Debe existir un conjunto de funciones que establezca cómo debe alcanzar la Agencia sus objetivos, pero permita cierta flexibilidad en su funcionamiento.

(13) La Agencia debe prestar asistencia a la Comisión mediante asesoramiento, dictámenes y análisis en todos los asuntos de la Unión relacionados con la formulación de políticas y disposiciones legislativas, actualizaciones y revisiones en el ámbito de la ciberseguridad, con inclusión de la protección de infraestructuras críticas y la ciberresiliencia. La Agencia debe actuar como punto de referencia de asesoramiento y conocimientos para la política y las iniciativas legislativas sectoriales de la Unión, cuando intervengan cuestiones relacionadas con la ciberseguridad.

(14) El cometido subyacente de la Agencia es promover la aplicación coherente del marco jurídico pertinente, en particular la aplicación efectiva de la Directiva SRI, que es esencial para aumentar la ciberresiliencia. Habida cuenta de la constante evolución de las amenazas para la ciberseguridad, es evidente que los Estados miembros deben estar respaldados por un enfoque más global y transversal en lo que se refiere a la creación de ciberresiliencia.

(15) La Agencia debe asistir a los Estados miembros y a las instituciones, órganos y organismos de la Unión en sus esfuerzos por conformar y mejorar su capacidad y preparación para prevenir, detectar y dar respuesta a los problemas e incidentes de ciberseguridad, así como en relación con la seguridad de las redes y los sistemas de

información. En particular, la Agencia debe prestar apoyo al desarrollo y potenciación de los CSIRT nacionales, con vistas a que alcancen un elevado nivel común de madurez en la Unión. La Agencia debe también prestar asistencia en la elaboración y actualización de las estrategias de los Estados miembros y de la Unión en materia de seguridad de las redes y los sistemas de información, y en particular de ciberseguridad, promover su difusión y hacer un seguimiento de los avances en su aplicación. La Agencia debe ofrecer asimismo cursos y material de formación a los organismos públicos y, cuando proceda, «formar formadores» con el fin de ayudar a los Estados miembros a desarrollar sus propias capacidades de formación.

(16) La Agencia debe asistir al Grupo de cooperación establecido en la Directiva SRI en la ejecución de sus tareas, en particular ofreciendo asesoramiento y consejo y facilitando el intercambio de mejores prácticas, particularmente con respecto a la identificación de los operadores de servicios esenciales por parte de los Estados miembros, en especial en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes.

(17) Con el fin de estimular la cooperación entre los sectores público y privado y dentro del sector privado, y en particular para apoyar la protección de las infraestructuras críticas, la Agencia debe facilitar la creación de centros sectoriales de puesta en común y análisis de la información (ISAC, por sus siglas en inglés), proporcionando directrices y mejores prácticas sobre las herramientas disponibles y los procedimientos, y orientando sobre la manera de abordar los asuntos normativos relacionados con la puesta en común de la información.

(18) La Agencia debe agregar y analizar los informes nacionales de los CSIRT y el CERT-UE y establecer unas normas, un lenguaje y una terminología comunes para el intercambio de información. Debe también fomentar la participación del sector privado, en el marco de la Directiva SRI, que estableció las bases para el intercambio voluntario de información técnica a nivel operativo con la creación de la red de CSIRT.

(19) La Agencia debe contribuir a aportar una respuesta a nivel de la UE en caso de incidentes y crisis de ciberseguridad transfronterizos a gran escala. Esta función debe incluir la recogida de información pertinente y el desempeño del papel de mediador entre la red de CSIRT y la comunidad técnica, así como los responsables políticos de gestionar la crisis. Por otra parte, la Agencia podría apoyar la gestión de incidentes desde una perspectiva técnica facilitando el intercambio de soluciones técnicas pertinentes entre los Estados miembros y aportando información a las comunicaciones públicas. La Agencia debe apoyar el proceso ensayando modalidades de esta cooperación a través de ejercicios anuales de ciberseguridad.

(20) Para llevar a cabo sus tareas operativas, la Agencia debe hacer uso de las competencias disponibles del CERT-UE a través de una cooperación estructurada, en estrecha proximidad física. La cooperación estructurada facilitará las sinergias necesarias y permitirá acumular conocimientos a ENISA. Cuando proceda, deben establecerse disposiciones específicas adecuadas entre las dos organizaciones para definir los aspectos prácticos de dicha cooperación.

(21) En cumplimiento de sus tareas operativas, la Agencia debe poder prestar ayuda a los Estados miembros, por ejemplo, mediante asesoramiento, asistencia técnica o análisis de amenazas e incidentes. La Recomendación de la Comisión sobre la respuesta coordinada a las crisis e incidentes de ciberseguridad a gran escala recomienda que los Estados miembros cooperen de buena fe y compartan entre ellos y con ENISA

información sobre las crisis e incidentes de ciberseguridad a gran escala sin demora indebida. Dicha información debe servir de ayuda a ENISA en el desempeño de sus funciones operativas.

(22) Dentro de la cooperación regular a nivel técnico para ayudar a la Unión a conocer la situación, la Agencia debe elaborar periódicamente el informe técnico de ciberseguridad de la UE sobre incidentes y amenazas, basándose en la información públicamente disponible, en su propio análisis y en los informes compartidos por los CSIRT de los Estados miembros (voluntariamente) o los puntos de contacto únicos de la Directiva SRI, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y, cuando proceda, el Centro de Inteligencia de la Unión Europea (INTCEN) del Servicio Europeo de Acción Exterior (SEAE). El informe debe ponerse a disposición de las instancias pertinentes del Consejo, la Comisión, la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y la red de CSIRT.

(23) Las investigaciones técnicas *ex post* en relación con incidentes con efectos significativos en más de un Estado miembro respaldadas o efectuadas por la Agencia a petición o con el acuerdo de los Estados miembros afectados deben centrarse en la prevención de incidentes futuros y llevarse a cabo sin perjuicio de eventuales procedimientos judiciales o administrativos destinados a determinar culpas o responsabilidades.

(24) Los Estados miembros afectados deben proporcionar a la Agencia la información y asistencia necesarias a efectos de la investigación, sin perjuicio de lo dispuesto en el artículo 346 del Tratado de Funcionamiento de la Unión Europea u otras razones de interés público.

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

(26) Para comprender mejor los retos en el campo de la ciberseguridad, y con el fin de facilitar asesoramiento estratégico a largo plazo a los Estados miembros y las instituciones de la Unión, la Agencia necesita analizar los riesgos actuales y emergentes. A tal efecto, la Agencia, en cooperación con los Estados miembros y, si procede, con los organismos estadísticos o de otro tipo, debe recopilar la información pertinente y llevar a cabo análisis de las tecnologías emergentes y proporcionar evaluaciones temáticas sobre los efectos jurídicos, económicos, sociales y reglamentarios que se esperan de las innovaciones tecnológicas sobre la seguridad de las redes y de la información, en particular la ciberseguridad. Además, la Agencia debe apoyar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a la hora de detectar nuevas tendencias y prevenir los problemas relacionados con la ciberseguridad, mediante la realización de análisis de amenazas e incidentes.

(27) Con el fin de aumentar la resiliencia de la Unión, la Agencia debe desarrollar la excelencia en el ámbito de la seguridad de la infraestructura de internet y de las infraestructuras críticas, ofreciendo asesoramiento, directrices y mejores prácticas. Con el fin de facilitar el acceso a una información mejor estructurada sobre los riesgos para la ciberseguridad y las posibles soluciones, la Agencia debe crear y mantener la «plataforma de información» de la Unión, un portal único con información sobre ciberseguridad para los ciudadanos procedente de las instituciones, órganos y organismos nacionales y de la UE.

(28) La Agencia debe contribuir a la sensibilización del público sobre los riesgos para la ciberseguridad y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos y organizaciones. Debe contribuir asimismo a promover las mejores prácticas y soluciones a nivel de personas y organizaciones mediante la recogida y análisis de la información disponible públicamente relativa a incidentes significativos y la elaboración de informes con vistas a ofrecer orientaciones a empresas y ciudadanos y mejorar el nivel general de preparación y resiliencia. La Agencia debe además, en colaboración con los Estados miembros y las instituciones, órganos y organismos de la Unión, organizar campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y a concienciar sobre las amenazas potenciales en el ciberespacio, incluyendo ciberdelitos como los ataques por suplantación de identidad (*phishing*), las redes infectadas (*botnets*) o los fraudes bancarios y financieros, así como dar consejos básicos en materia de autenticación y protección de datos. La Agencia debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos.

(29) Con el fin de apoyar a las empresas que trabajan en el sector de la ciberseguridad, así como a los usuarios de soluciones de ciberseguridad, la Agencia debe crear y mantener un «observatorio del mercado», llevando a cabo análisis y difundiendo las principales tendencias en el mercado de la ciberseguridad, tanto en el lado de la oferta como en el de la demanda.

(30) Para asegurar que cumple plenamente sus objetivos, la Agencia debe permanecer en contacto con las instituciones, órganos y organismos pertinentes, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Agencia Europea de Defensa (AED), la Agencia europea para la gestión operativa de los sistemas informáticos de gran magnitud (eu-LISA), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la UE relacionado con la ciberseguridad. También debe mantener contactos con las autoridades encargadas de la protección de datos a fin de intercambiar conocimientos y mejores prácticas y facilitar asesoramiento sobre los aspectos de la ciberseguridad que podrían repercutir en su trabajo. Los representantes de las autoridades nacionales y de la Unión encargadas de hacer cumplir la ley y proteger los datos deben poder estar representados en el Grupo Permanente de Partes Interesadas de la Agencia. En sus relaciones con los organismos encargados de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en el trabajo de dichos organismos, la Agencia debe respetar los canales de información y las redes existentes.

(31) La Agencia, como miembro de la red de CSIRT que además se encarga de su secretaría, debe prestar apoyo a los CSIRT de los Estados miembros y al CERT-UE en la cooperación operativa relativa a todas las tareas pertinentes de la red de CSIRT, tal como se definen en la Directiva SRI. Además, la Agencia debe promover y apoyar la cooperación entre los CSIRT pertinentes en caso de incidentes, ataques o perturbaciones en las redes o infraestructuras gestionadas o protegidas por los CSIRT y que impliquen o puedan implicar al menos a dos CERT, teniendo siempre debidamente en cuenta los procedimientos operativos estándar de la red de CSIRT.

(32) Con el fin de aumentar la preparación de la Unión para una respuesta a los incidentes de ciberseguridad, la Agencia debe organizar anualmente ejercicios de ciberseguridad a nivel de la Unión y, cuando lo soliciten, apoyar a los Estados miembros y las instituciones, órganos y organismos de la UE en la organización de ejercicios.

(33) La Agencia debe desarrollar y mantener sus conocimientos técnicos en materia de certificación de la ciberseguridad con vistas a respaldar la política de la Unión en este ámbito. Debe igualmente promover la asimilación de la certificación de la ciberseguridad en la Unión, en particular contribuyendo a la creación y mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.

(34) Unas políticas de ciberseguridad eficientes deben basarse en métodos de evaluación de riesgos bien desarrollados, tanto en el sector público como en el privado. Los métodos de evaluación de riesgos se utilizan en distintos niveles sin que existan prácticas comunes para su aplicación eficiente. La promoción y el desarrollo de las mejores prácticas de evaluación de riesgos y de soluciones interoperables de gestión de riesgos en las organizaciones de los sectores público y privado incrementarán el nivel de ciberseguridad en la Unión. A tal efecto, la Agencia debe apoyar la cooperación entre las partes interesadas a escala de la Unión, facilitando sus esfuerzos en relación con el establecimiento y la adopción de normas a escala europea e internacional para la gestión del riesgo y la seguridad mensurable de los productos, sistemas, redes y servicios electrónicos que, junto a los programas informáticos, conforman las redes y los sistemas de información.

(35) La Agencia debe alentar a los Estados miembros y a los proveedores de servicios a aumentar sus niveles generales de seguridad, a fin de que todos los usuarios de internet puedan tomar las medidas necesarias para garantizar su propia ciberseguridad personal. En particular, los prestadores de servicios y los fabricantes de productos deben retirar o reciclar los productos y servicios que no cumplan las normas de ciberseguridad. En cooperación con las autoridades competentes, ENISA podrá difundir información relativa al nivel de ciberseguridad de los productos y servicios ofrecidos en el mercado interior, y emitir advertencias dirigidas a los proveedores y los fabricantes solicitándoles que mejoren la seguridad, incluida la ciberseguridad, de sus productos y servicios.

(36) La Agencia debe tener plenamente en cuenta las actividades en curso de investigación, desarrollo y evaluación tecnológica, en especial las llevadas a cabo por las distintas iniciativas de investigación de la Unión, para asesorar a las instituciones, órganos y organismos de la Unión y, cuando proceda, a los Estados miembros que lo soliciten sobre las necesidades de investigación en el ámbito de la seguridad de las redes y de la información, y en particular de la ciberseguridad.

(37) Los problemas de ciberseguridad tienen un alcance mundial. Es necesaria una cooperación internacional más estrecha para mejorar las normas de seguridad, incluida la definición de normas de comportamiento comunes, y el intercambio de información, promoviendo una colaboración internacional que responda con mayor prontitud a los problemas de seguridad de las redes y de la información, así como un enfoque mundial común al respecto. A tal efecto, la Agencia debe respaldar una mayor relación y cooperación de la Unión con los terceros países y las organizaciones internacionales proporcionando, cuando proceda, los conocimientos y el análisis necesarios a las instituciones, órganos y organismos pertinentes de la Unión.

(38) La Agencia debe estar en condiciones de responder a las solicitudes específicas de asesoramiento y asistencia por parte de los Estados miembros y las instituciones, órganos y organismos de la UE que cuadren con los objetivos de la Agencia.

(39) Es necesario aplicar determinados principios al gobierno de la Agencia con el fin de atenerse a la declaración conjunta y el enfoque común aprobados en julio de 2012 por el Grupo de trabajo interinstitucional sobre las agencias descentralizadas, declaración y enfoque cuya finalidad es la racionalización las actividades de las agencias y la mejora de su rendimiento. La declaración conjunta y el enfoque común también han de quedar reflejados, cuando proceda, en los programas de trabajo de la Agencia, sus evaluaciones y sus prácticas administrativas y de presentación de informes.

(40) El Consejo de Administración, integrado por los Estados miembros y la Comisión, debe definir la orientación general del funcionamiento de la Agencia y garantizar que desempeña su cometido de conformidad con el presente Reglamento. El Consejo de Administración debe estar dotado de las facultades necesarias para establecer el presupuesto, supervisar su ejecución, aprobar el correspondiente reglamento financiero, establecer procedimientos de trabajo transparentes para la toma de decisiones por la Agencia, adoptar el documento único de programación de la Agencia, adoptar su propio reglamento interno, nombrar al director ejecutivo y decidir la prolongación del mandato del director ejecutivo o el cese de dicho mandato.

(41) Para que la Agencia funcione correcta y eficazmente, la Comisión y los Estados miembros deben garantizar que las personas que se nombren como miembros del Consejo de Administración dispongan de las competencias profesionales adecuadas y de experiencia en las áreas funcionales. La Comisión y los Estados miembros deben asimismo tratar de limitar la rotación de sus respectivos representantes en el Consejo de Administración, con el fin de garantizar la continuidad en su labor.

(42) En aras del buen funcionamiento de la Agencia, es preciso que su director ejecutivo sea nombrado atendiendo a sus méritos y a su capacidad administrativa y de gestión debidamente acreditada, así como a su competencia y experiencia en relación con la ciberseguridad. También es necesario que desempeñe sus funciones con completa independencia. El director ejecutivo debe preparar una propuesta de programa de trabajo de la Agencia, previa consulta con la Comisión, y tomar todas las medidas necesarias para garantizar la correcta ejecución de dicho programa de trabajo. El director ejecutivo debe preparar un informe anual, que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de la Agencia y ejecutar el presupuesto. Además, debe tener la posibilidad de crear grupos de trabajo *ad hoc* para que examinen asuntos concretos, en particular los de índole científica, técnica o jurídica o socioeconómica. El director ejecutivo debe garantizar que los miembros de los grupos de trabajo *ad hoc* sean seleccionados entre los expertos de mayor nivel, teniendo debidamente en cuenta la necesidad de lograr un equilibrio representativo, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información.

(43) El Comité Ejecutivo debe contribuir al buen funcionamiento del Consejo de Administración. Como parte de sus trabajos preparatorios relativos a las decisiones del Consejo de Administración, debe examinar en detalle la información pertinente, explorar las opciones disponibles y ofrecer asesoramiento y soluciones para preparar las decisiones pertinentes del Consejo de Administración.

(44) La Agencia debe contar con un Grupo Permanente de Partes Interesadas en calidad de organismo consultivo, a fin de garantizar un diálogo sistemático con el sector privado, las organizaciones de consumidores y otras partes interesadas pertinentes. El Grupo

Permanente de Partes Interesadas, establecido por el Consejo de Administración a propuesta del director ejecutivo, debe centrarse en cuestiones que afecten a las partes interesadas y ponerlas en conocimiento de la Agencia. La composición del Grupo Permanente de Partes Interesadas y las tareas asignadas a este grupo, que debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo, deben garantizar una representación suficiente de las partes interesadas en los trabajos de la Agencia.

(45) La Agencia instaurará normas para la prevención y gestión de los conflictos de intereses. La Agencia debe aplicar asimismo las disposiciones pertinentes de la Unión relativas al acceso del público a los documentos, según establece el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo[34]. Los datos personales deben ser tratados por la Agencia de conformidad con el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[35]. La Agencia debe cumplir las disposiciones aplicables a las instituciones de la Unión, así como la legislación nacional en materia de tratamiento de la información, en particular la información sensible no clasificada y la información clasificada de la UE.

(46) Con el fin de garantizar la plena autonomía e independencia de la Agencia y para que pueda desempeñar funciones adicionales y nuevas, incluidas tareas de emergencia imprevistas, se considera necesario concederle un presupuesto suficiente y autónomo cuyos ingresos procedan principalmente de una contribución de la Unión y de contribuciones de los terceros países que participen en los trabajos de la Agencia. La mayor parte del personal de la Agencia debe estar dedicado directamente a la aplicación operativa de su mandato. Debe permitirse que el Estado miembro que la acoge, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de la Agencia. El procedimiento presupuestario de la Unión debe seguir siendo aplicable por lo que respecta a las subvenciones imputables al presupuesto general de la Unión. Además, el Tribunal de Cuentas Europeo debe realizar una auditoría de las cuentas de la Agencia para garantizar la transparencia y la responsabilidad.

(47) La evaluación de la conformidad es el proceso por el que se demuestra que se han cumplido los requisitos especificados para un producto, proceso, servicio, sistema, persona u organismo. A efectos del presente Reglamento, la certificación debe ser considerada un tipo de evaluación de la conformidad relativa a las características de ciberseguridad de un producto, proceso, servicio, sistema, o combinación de estos («productos y servicios de TIC») por un tercero independiente, distinto del fabricante del producto o del prestador de servicios. La certificación no puede garantizar por sí misma la ciberseguridad de los productos y servicios de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos y servicios de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

---

34 Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

35 DO L 8 de 12.1.2001, p. 1.

(48) La certificación de la ciberseguridad desempeña un importante papel a la hora de aumentar la confianza y la seguridad en los productos y servicios de TIC. El mercado único digital, y en particular la economía de los datos y la internet de las cosas, solo pueden prosperar si el público en general confía en que dichos productos y servicios ofrecen un determinado nivel de garantía de ciberseguridad. Los vehículos conectados y automatizados, los dispositivos médicos electrónicos, los sistemas de control de la automatización industrial o las redes inteligentes son solo algunos ejemplos de sectores en los que la certificación se utiliza ya ampliamente o es probable que se utilice en un futuro próximo. También en los sectores regulados por la Directiva SRI resulta crítica la certificación de la ciberseguridad.

(49) En la Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora», la Comisión indicó la necesidad de productos y soluciones de ciberseguridad de alta calidad, asequibles e interoperables. El suministro de los productos y servicios de TIC dentro del mercado único sigue estando muy fragmentado desde el punto de vista geográfico. Esto se debe a que la industria de la ciberseguridad en Europa se ha desarrollado en gran medida a partir de la demanda de los gobiernos nacionales. Además, la falta de soluciones interoperables (normas técnicas), prácticas y mecanismos de certificación a escala de la UE es otra de las carencias que padece el mercado único de la ciberseguridad. Por una parte, esto hace difícil que las empresas europeas compitan a nivel nacional, europeo y mundial; por otra, reduce las opciones de contar con tecnologías de ciberseguridad viables y utilizables a las que puedan acceder particulares y empresas. Del mismo modo, en la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital, la Comisión destacó la necesidad de seguridad en los productos y sistemas conectados, indicando que la creación de un marco europeo de seguridad de las TIC que establezca pautas para organizar la certificación de seguridad de las TIC en la Unión podría tanto preservar la confianza en internet como combatir la actual fragmentación del mercado de la ciberseguridad.

(50) En la actualidad, la certificación de la ciberseguridad de los productos y servicios de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de regímenes impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos y servicios en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales. Por otra parte, aun cuando están surgiendo nuevos regímenes, no parece haber un planteamiento coherente y holístico con respecto a las cuestiones horizontales relacionadas con la ciberseguridad, por ejemplo en el ámbito de la internet de las cosas. Los regímenes existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real.

(51) Se han realizado esfuerzos en el pasado para propiciar el reconocimiento mutuo de los certificados en Europa, pero solo han tenido un éxito parcial. El ejemplo más importante a este respecto es el Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS). Si bien constituye el modelo más importante para la cooperación y el reconocimiento mutuo en el ámbito de la certificación de la seguridad, el ARM del SOG-IS presenta algunas deficiencias importantes relacionadas con su elevado coste y limitado alcance. Hasta la fecha, solo se ha desarrollado un corto número de perfiles de protección para

productos digitales tales como la firma digital, el tacógrafo digital y las tarjetas inteligentes. Y lo que es más importante, el SOG-IS incluye solo a una parte de los Estados miembros de la Unión. Esto ha limitado la eficacia del ARM del SOG-IS desde el punto de vista del mercado interior.

(52) Por todo ello, es necesario establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar regímenes europeos de certificación de la ciberseguridad y permita que los certificados de productos y servicios de TIC sean reconocidos y usados en todos los Estados miembros. El marco europeo debe tener un doble objetivo: por una parte, contribuir a aumentar la confianza en los productos y servicios de TIC que hayan sido certificados con arreglo a tales regímenes; por otra, evitar la multiplicación de certificaciones nacionales de la ciberseguridad contradictorias o redundantes y, por ende, reducir los costes para las empresas que operan en el mercado único digital. Los regímenes deben ser no discriminatorios y basarse en normas internacionales o de la Unión, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la UE al respecto.

(53) La Comisión debe estar facultada para adoptar regímenes europeos de certificación de la ciberseguridad relativos a grupos específicos de productos y servicios de TIC. Estos regímenes deben ser implantados y supervisados por las autoridades nacionales de supervisión de la certificación y los certificados expedidos con arreglo a ellos deben ser válidos y reconocidos en toda la Unión. Los regímenes de certificación operados por el sector industrial u otras organizaciones privadas deben quedar fuera del ámbito de aplicación del Reglamento. No obstante, los organismos responsables de dichos regímenes podrán proponer a la Comisión que los tome en consideración como base para su aprobación como regímenes europeos.

(54) Las disposiciones del presente Reglamento deben entenderse sin perjuicio de la legislación de la Unión que fija normas específicas sobre la certificación de productos y servicios de TIC. En particular, el Reglamento general de protección de datos (RGPD) establece disposiciones para implantar mecanismos de certificación y sellos y marcas de protección de datos a fin de demostrar la conformidad con ese Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. Estos mecanismos de certificación y sellos y marcas de protección de datos deben permitir a los interesados evaluar rápidamente el nivel de protección de datos de los correspondientes productos y servicios. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del RGPD, incluso cuando dichas operaciones se encuentran integradas en productos y servicios.

(55) El objetivo de los regímenes europeos de certificación de la ciberseguridad debe ser garantizar que los productos y servicios de TIC certificados con arreglo a un régimen cumplan los requisitos especificados. Tales requisitos se refieren a la capacidad de resistir, con un nivel determinado de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, procesos, servicios y sistemas, en el sentido del presente Reglamento, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle en el presente Reglamento los requisitos de ciberseguridad relativos a todos los productos y servicios de TIC. Los productos y servicios de TIC y las correspondientes necesidades de ciberseguridad son tan dispares que es muy difícil presentar unos requisitos de ciberseguridad generales de validez global. Por lo tanto, es necesario adoptar un

concepto amplio y general de la ciberseguridad a efectos de la certificación, complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los regímenes europeos de certificación de la ciberseguridad. Las modalidades con que se lograrán tales objetivos para determinados productos y servicios de TIC deben especificarse luego con más detalle a nivel de cada régimen de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas.

(56) La Comisión debe estar facultada para solicitar a ENISA que prepare propuestas de regímenes para productos o servicios de TIC específicos. A continuación, la Comisión, sobre la base de las propuestas presentadas por ENISA, debe estar facultada para adoptar el régimen europeo de certificación de la ciberseguridad mediante actos de ejecución. Teniendo en cuenta la finalidad general y los objetivos de seguridad definidos en el presente Reglamento, los regímenes europeos de certificación de la ciberseguridad adoptados por la Comisión deben especificar un conjunto mínimo de elementos relacionados con el objeto, alcance y funcionamiento del régimen concreto. Entre ellos deben figurar el alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos y servicios de TIC que cubre, la especificación detallada de los requisitos de ciberseguridad, por ejemplo haciendo referencia a normas o especificaciones técnicas, los criterios y métodos de evaluación específicos, así como el nivel de garantía: básico, sustancial o elevado.

(57) El recurso a la certificación europea de la ciberseguridad debe seguir siendo voluntario, salvo que se prevea otra cosa en la legislación nacional o de la Unión. No obstante, con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los regímenes o procedimientos nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos por un régimen europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de la fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos regímenes nacionales de certificación de la ciberseguridad para productos y servicios de TIC cubiertos ya por un régimen europeo existente.

(58) Una vez que se adopte un régimen europeo de certificación de la ciberseguridad, los fabricantes de productos de TIC o proveedores de servicios de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios al organismo de evaluación de la conformidad que prefieran. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos de acreditación deben revocar la acreditación de un organismo de evaluación de la conformidad cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

(59) Es necesario exigir a todos los Estados miembros que designen a una autoridad de supervisión de la certificación de la ciberseguridad para supervisar el cumplimiento, por parte de los organismos de evaluación de la conformidad establecidos en su territorio y de los certificados por ellos expedidos, de los requisitos del presente Reglamento y de los regímenes de certificación de la ciberseguridad pertinentes. Las autoridades nacionales de supervisión de la certificación deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los

certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigar el asunto objeto de la reclamación en la medida que proceda e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable. Además, deben cooperar con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los requisitos del presente Reglamento o de regímenes de ciberseguridad específicos.

(60) Con vistas a garantizar una aplicación coherente del marco europeo de certificación de la ciberseguridad, debe establecerse un Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»), constituido por las autoridades nacionales de supervisión de la certificación. Los cometidos principales del Grupo deben ser asesorar y asistir a la Comisión en su labor de garantizar una implantación y aplicación coherentes del marco europeo de certificación de la ciberseguridad; asistir y cooperar estrechamente con la Agencia en la preparación de las propuestas de regímenes de certificación de la ciberseguridad; recomendar que la Comisión solicite a la Agencia que prepare una propuesta de régimen europeo de certificación de la ciberseguridad; y adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los regímenes europeos de certificación de la ciberseguridad existentes.

(61) Con el fin de reforzar la sensibilización y facilitar la aceptación de los futuros regímenes de ciberseguridad de la UE, la Comisión Europea podrá formular directrices generales o sectoriales en materia de ciberseguridad, por ejemplo, sobre buenas prácticas de ciberseguridad o sobre comportamiento responsable en materia de ciberseguridad, destacando el efecto positivo de la utilización de productos y servicios TIC certificados.

(62) La ayuda prestada por la Agencia a la certificación de la ciberseguridad debe incluir también los contactos con el Comité de Seguridad del Consejo y el organismo nacional pertinente, en relación con la aprobación criptográfica de los productos para su uso en redes clasificadas.

(63) A fin de precisar los criterios para la acreditación de los organismos de evaluación de la conformidad, deben delegarse en la Comisión los poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. La Comisión debe llevar a cabo las oportunas consultas durante sus trabajos preparatorios, también a nivel de expertos. Dichas consultas deben realizarse de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016. En particular, para garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(64) A fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011.

(65) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los regímenes europeos de certificación de la ciberseguridad de productos y

servicios de TIC, sobre las modalidades de ejecución de las investigaciones por parte de la Agencia y sobre las circunstancias, formatos y procedimientos de notificación a la Comisión por parte de los organismos de evaluación de la conformidad acreditados por las autoridades nacionales de supervisión de la certificación.

(66) Las actividades de la Agencia deben evaluarse de modo independiente. La evaluación debe tener en cuenta el logro de sus objetivos por parte de la Agencia, sus prácticas de trabajo y la pertinencia de sus tareas. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad.

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

(68) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que pueden lograrse mejor a nivel 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 enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto y ámbito de aplicación

Con vistas a garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a un nivel elevado de ciberseguridad, ciberrresiliencia y confianza dentro de la Unión, el presente Reglamento:

a) establece los objetivos, funciones y aspectos organizativos de ENISA, la «Agencia de Ciberseguridad de la UE», denominada en lo sucesivo «la Agencia»; y

b) establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos y servicios de TIC en la Unión. Dicho marco se aplicará sin perjuicio de las disposiciones específicas relativas a la certificación de carácter voluntario u obligatorio contenidas en otros actos de la Unión.

Artículo 2
Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «ciberseguridad», todas las actividades necesarias para la protección de las redes y sistemas de información, de sus usuarios y de las personas afectadas por las ciberamenazas;

2) «redes y sistemas de información», un sistema en el sentido del artículo 4, punto 1, de la Directiva (UE) 2016/1148;

3) «estrategia nacional de seguridad de las redes y sistemas de información», un marco en el sentido del artículo 4, punto 3, de la Directiva (UE) 2016/1148;

4) «operador de servicios esenciales», una entidad pública o privada según se define en el artículo 4, punto 4, de la Directiva (UE) 2016/1148;

5) «proveedor de servicios digitales», una persona jurídica que presta un servicio digital según se define en el artículo 4, punto 6, de la Directiva (UE) 2016/1148;

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

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

8) «ciberamenaza», cualquier circunstancia potencial o hecho que pueda afectar desfavorablemente a las redes y los sistemas de información, a sus usuarios y a las personas afectadas;

9) «régimen europeo de certificación de la ciberseguridad», conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos definidos a nivel de la Unión aplicables a la certificación de los productos y servicios de tecnologías de la información y la comunicación (TIC) incluidos en el ámbito de aplicación de dicho régimen específico;

10) «certificado europeo de ciberseguridad», documento expedido por un organismo de evaluación de la conformidad que certifica que determinado producto o servicio de TIC cumple los requisitos específicos establecidos en un régimen europeo de certificación de la ciberseguridad;

11) «producto y servicio de TIC», todo elemento o grupo de elementos de las redes y los sistemas de información;

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

13) «organismo nacional de acreditación», un organismo nacional de acreditación tal como se define en el artículo 2, punto 11, del Reglamento (CE) n.º 765/2008;

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

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

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

TÍTULO II
ENISA – la «Agencia de Ciberseguridad de la UE»

CAPÍTULO I
MANDATO, OBJETIVOS Y TAREAS

Artículo 3
Mandato

1. La Agencia desempeñará los cometidos que le asigna el presente Reglamento con el fin de contribuir a un elevado nivel de ciberseguridad dentro de la Unión.

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

3. Los objetivos y cometidos de la Agencia se entenderán sin perjuicio de las competencias de los Estados miembros en materia de ciberseguridad y, en todo caso, sin perjuicio de las actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

Artículo 4
Objetivos

1. La Agencia será un centro de conocimientos técnicos sobre ciberseguridad en virtud de su independencia, la calidad científica y técnica del asesoramiento y la asistencia prestados y la información ofrecida, la transparencia de sus procedimientos operativos y métodos de funcionamiento y su diligencia en el desempeño de sus funciones.

2. La Agencia asistirá a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas relativas a la ciberseguridad.

3. La Agencia prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a la Unión, los Estados miembros y las partes interesadas públicas y privadas a fin de incrementar la protección de sus redes y sistemas de información, desarrollar las capacidades y competencias en el ámbito de la ciberseguridad y lograr la ciberresiliencia.

4. La Agencia fomentará la cooperación y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, incluido el sector privado, sobre las cuestiones relacionadas con la ciberseguridad.

5. La Agencia incrementará las capacidades de ciberseguridad a nivel de la Unión para complementar la acción de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

6. La Agencia promoverá el uso de la certificación, en particular contribuyendo a la creación y el mantenimiento de un marco de certificación de la ciberseguridad a nivel de la Unión de conformidad con el título III del presente Reglamento, con el fin de

aumentar la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC y reforzar así la confianza en el mercado interior digital.

7. La Agencia promoverá un alto nivel de sensibilización de los ciudadanos y empresas en torno a las cuestiones relacionadas con la ciberseguridad.

Artículo 5

Tareas relativas al desarrollo y ejecución de la política y la legislación de la Unión

La Agencia contribuirá al desarrollo y ejecución de la política y la legislación de la Unión:

1. Prestando asistencia y asesoramiento, en particular emitiendo su dictamen independiente y aportando trabajos preparatorios, en el desarrollo y la revisión de la política y la legislación de la Unión en el ámbito de la ciberseguridad, así como las iniciativas políticas y legislativas sectoriales cuando estén presentes cuestiones relacionadas con la ciberseguridad.

2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y la legislación de la Unión en materia de ciberseguridad, especialmente en relación con la Directiva (UE) 2016/1148, en particular a través de dictámenes, directrices, recomendaciones y mejores prácticas sobre temas como la gestión de riesgos, la notificación de incidentes y la comunicación de información, así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto.

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

4. Respaldando:

    1) el desarrollo y la aplicación de la política de la Unión en el ámbito de la identidad electrónica y los servicios de confianza, en particular ofreciendo asesoramiento y directrices técnicas y facilitando el intercambio de mejores prácticas entre las autoridades competentes;

    2) la promoción de una mejora del nivel de seguridad de las comunicaciones electrónicas, en particular ofreciendo asistencia y asesoramiento y facilitando el intercambio de mejores prácticas entre las autoridades competentes.

5. Respaldando la revisión periódica de las actividades políticas de la Unión mediante la preparación de un informe anual sobre el estado de la aplicación del marco jurídico respectivo en relación con:

    a) las notificaciones de incidentes de los Estados miembros suministradas por el punto de contacto único al Grupo de cooperación de conformidad con el artículo 10, apartado 3, de la Directiva (UE) 2016/1148;

    b) las notificaciones de violación de la seguridad y pérdida de la integridad respecto de los proveedores de servicios de confianza, suministradas por los organismos de supervisión a la Agencia de conformidad con el artículo 19, apartado 3, del Reglamento (UE) n.º 910/2014;

    c) las notificaciones de violación de la seguridad transmitidas por las empresas suministradoras de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, suministradas por las

autoridades competentes a la Agencia de conformidad con el artículo 40 de la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas].

Artículo 6
Tareas relativas a la creación de capacidades

1. La Agencia asistirá:

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

b) a las instituciones, órganos y organismos de la Unión en sus esfuerzos para mejorar la prevención, detección, análisis y capacidad de respuesta a problemas e incidentes de ciberseguridad a través de un apoyo adecuado al CERT de las instituciones, órganos y organismos de la Unión (CERT-UE);

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

d) a los Estados miembros, a petición suya, en el desarrollo de estrategias nacionales sobre seguridad de las redes y los sistemas de información, con arreglo al artículo 7, apartado 2, de la Directiva (UE) 2016/1148; la Agencia también promoverá la difusión y el seguimiento de los progresos en la aplicación de estas estrategias en toda la Unión, con el fin de promover las mejores prácticas;

e) a las instituciones de la Unión en la elaboración y revisión de las estrategias de la Unión en materia de ciberseguridad, promoviendo la difusión y el seguimiento de los progresos en su aplicación;

f) a los CSIRT nacionales y de la Unión para elevar el nivel de sus capacidades, en particular promoviendo el diálogo y el intercambio de información, con el fin de lograr que, habida cuenta de los avances más recientes, cada CSIRT disponga de un conjunto mínimo de capacidades y se atenga a las mejores prácticas;

g) a los Estados miembros, organizando cada año los ejercicios de ciberseguridad a gran escala a nivel de la Unión a que se refiere el artículo 7, apartado 6, y formulando recomendaciones políticas basadas en el proceso de evaluación de los ejercicios y en las enseñanzas extraídas de ellos;

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

i) al Grupo de cooperación, mediante el intercambio de mejores prácticas, en particular con respecto a la identificación de los operadores de servicios esenciales por parte de los Estados miembros, especialmente en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes, con arreglo al artículo 11, apartado 3, letra l), de la Directiva (UE) 2016/1148.

2. La Agencia facilitará el establecimiento de centros sectoriales de puesta en común y análisis de la información (ISAC) y les prestará un apoyo continuado, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, aportando

mejores prácticas y orientaciones sobre las herramientas disponibles, el procedimiento y la manera de abordar los asuntos normativos relacionados con el intercambio de información.

Artículo 7

Tareas relativas a la cooperación operativa a nivel de la Unión

1. La Agencia apoyará la cooperación operativa entre los organismos públicos competentes y entre las partes interesadas.

2. La Agencia cooperará a nivel operativo y establecerá sinergias con las instituciones, órganos y organismos de la Unión, incluido el CERT-UE, los servicios que abordan la ciberdelincuencia y las autoridades responsables de la protección de la intimidad y los datos personales, con vistas a tratar cuestiones de interés común, en particular mediante:

   a) el intercambio de conocimientos técnicos y mejores prácticas;

   b) la prestación de asesoramiento y directrices sobre cuestiones de interés relacionadas con la ciberseguridad;

   c) el establecimiento, previa consulta de la Comisión, de disposiciones prácticas para la ejecución de tareas específicas.

3. La Agencia se hará cargo de la secretaría de la red de CSIRT, de conformidad con el artículo 12, apartado 2, de la Directiva (UE) 2016/1148, y facilitará activamente el intercambio de información y la cooperación entre sus miembros.

4. La Agencia contribuirá a la cooperación operativa dentro de la red de CSIRT y prestará apoyo a los Estados miembros:

   a) asesorando sobre cómo mejorar su capacidad para prevenir, detectar y dar respuesta a los incidentes;

   b) proporcionando, previa solicitud, asistencia técnica en caso de incidentes con un impacto significativo o sustancial;

   c) analizando las vulnerabilidades, artefactos e incidentes.

En el desempeño de estas funciones, la Agencia y el CERT-UE entablarán una cooperación estructurada con el fin de beneficiarse de las sinergias, especialmente en lo que se refiere a los aspectos operativos.

5. A petición de dos o más Estados miembros afectados y con el único objetivo de prestar asesoramiento para la prevención de incidentes futuros, la Agencia prestará apoyo para que se realice, o realizará, una investigación técnica *ex post* tras las notificaciones por las empresas afectadas de incidentes que tengan un impacto significativo o sustancial con arreglo a la Directiva (UE) 2016/1148. La Agencia también llevará a cabo dicha investigación tras una solicitud debidamente justificada de la Comisión de acuerdo con los Estados miembros afectados en caso de incidentes que afecten a más de dos Estados miembros.

El alcance de la investigación y el procedimiento que debe seguirse para llevarla a cabo serán objeto de acuerdo entre los Estados miembros afectados y la Agencia, y se entenderá sin perjuicio de eventuales investigaciones penales relativas al mismo incidente. La investigación concluirá con un informe técnico final elaborado por la Agencia, en particular sobre la base de la información y las observaciones de los Estados miembros y empresa(s) afectados y consensuado con los Estados miembros afectados. Se ofrecerá a la red de CSIRT un resumen del informe centrado en las recomendaciones para la prevención de incidentes futuros.

6. La Agencia organizará anualmente ejercicios de ciberseguridad a nivel de la Unión y apoyará a los Estados miembros y a las instituciones, órganos y organismos de la UE en la organización de ejercicios a petición suya. Los ejercicios anuales a nivel de la Unión incluirán elementos técnicos, operativos y estratégicos y contribuirán a preparar la respuesta cooperativa a nivel de la Unión a los incidentes de ciberseguridad a gran escala y de carácter transfronterizo. La Agencia participará asimismo en la realización de ejercicios sectoriales de ciberseguridad, y contribuirá a organizarlos cuando proceda, junto con los ISAC pertinentes y permitirá a los ISAC participar también en los ejercicios de ciberseguridad a nivel de la Unión.

7. La Agencia elaborará un informe periódico sobre la situación técnica de la ciberseguridad en la UE, relativo a incidentes y amenazas, basándose en la información de fuentes abiertas, en su propio análisis y en los informes comunicados, entre otros, por los CSIRT de los Estados miembros (con carácter voluntario) o los puntos de contacto únicos de la Directiva SRI (de conformidad con su artículo 14, apartado 5), el Centro Europeo de Ciberdelincuencia (EC3) de Europol y el CERT-UE.

8. La Agencia contribuirá a desarrollar una respuesta cooperativa, a nivel de la Unión y de Estado miembro, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad, principalmente por los siguientes medios:

   a) agregación de los informes procedentes de fuentes nacionales, con vistas a contribuir a la creación de una perspectiva común de la situación;

   b) garantía de la eficacia del flujo de información y oferta de mecanismos de intensificación entre la red de CSIRT y los responsables políticos y técnicos a nivel de la Unión;

   c) apoyo a la gestión técnica de un incidente o crisis, en particular facilitando la puesta en común de soluciones técnicas entre los Estados miembros;

   d) apoyo a la comunicación pública en torno al incidente o crisis;

   e) ensayo de los planes de cooperación para responder a estos incidentes o crisis.

Artículo 8

Tareas relativas al mercado, certificación de la ciberseguridad y normalización

La Agencia:

a) Apoyará y promoverá el desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de productos y servicios de TIC, según lo establecido en el título III del presente Reglamento, por los siguientes medios:

1) preparar propuestas de regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC de conformidad con el artículo 44 del presente Reglamento;

2) asistir a la Comisión, encargándose de la secretaría del Grupo Europeo de Certificación de la Ciberseguridad de conformidad con el artículo 53 del presente Reglamento;

3) recopilar y publicar directrices y desarrollar buenas prácticas relativas a los requisitos de ciberseguridad de los productos y servicios de TIC, en cooperación con las autoridades nacionales de supervisión de la certificación y con la industria.

b) Facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos y servicios de TIC y elaborará, en colaboración con los Estados miembros, directrices y orientaciones relativas a las áreas técnicas relacionadas con los requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, así como relativas a normas ya existentes, entre ellas las normas nacionales de los Estados miembros, con arreglo al artículo 19, apartado 2, de la Directiva (UE) 2016/1148.

c) Realizará y difundirá análisis periódicos de las principales tendencias en el mercado de la ciberseguridad, tanto del lado de la oferta como de la demanda, con el fin de fomentar dicho mercado en la Unión.

Artículo 9

Tareas relativas al conocimiento, la información y la sensibilización

La Agencia:

a) efectuará análisis de las tecnologías emergentes y preparará evaluaciones temáticas sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas sobre la ciberseguridad;

b) realizará análisis estratégicos a largo plazo de las amenazas e incidentes de ciberseguridad, con el fin de detectar las tendencias emergentes y ayudar a prevenir los problemas relacionados con la ciberseguridad;

c) aportará, en cooperación con los expertos de las autoridades de los Estados miembros, dictámenes, directrices y mejores prácticas para la seguridad de las redes y los sistemas de información, en particular en el ámbito de la seguridad de la infraestructura de internet y de las infraestructuras que sustentan los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148;

d) reunirá, organizará y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión;

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

f) recopilará y analizará la información disponible públicamente relativa a incidentes significativos y elaborará informes con el fin de ofrecer orientaciones a las empresas y ciudadanos de toda la Unión;

g) organizará, en cooperación con los Estados miembros y las instituciones, órganos y organismos de la Unión, campañas periódicas de divulgación para aumentar la ciberseguridad y su visibilidad en la Unión.

Artículo 10
Tareas relativas a la investigación y la innovación

En relación con la investigación y la innovación, la Agencia:

a) asesorará a la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad, con miras a poder ofrecer respuestas eficaces a los riesgos y amenazas actuales y futuros, también en relación con las tecnologías de la información y la comunicación nuevas y emergentes, y a utilizar eficazmente las tecnologías de prevención del riesgo;

b) participará, cuando la Comisión le haya delegado los poderes correspondientes, en la fase de ejecución de los programas de financiación de la investigación y la innovación, o en calidad de beneficiario.

Artículo 11
Tareas relativas a la cooperación internacional

La Agencia contribuirá a los esfuerzos de la Unión por cooperar con terceros países y organizaciones internacionales a fin de promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad, por los siguientes medios:

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

b) facilitar, a petición de la Comisión, el intercambio de mejores prácticas entre las organizaciones internacionales pertinentes;

c) facilitar asesoramiento a la Comisión cuando así se solicite.

CAPÍTULO II
ORGANIZACIÓN DE LA AGENCIA

Artículo 12
Estructura

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

a) un Consejo de Administración, que ejercerá las funciones definidas en el artículo 14;

b) un Comité Ejecutivo, que ejercerá las funciones definidas en el artículo 18;

c) un director ejecutivo, con las responsabilidades definidas en el artículo 19; y

d) un Grupo Permanente de Partes Interesadas, que ejercerá las funciones definidas en el artículo 20.

SECCIÓN 1
CONSEJO DE ADMINISTRACIÓN

Artículo 13
Composición del Consejo de Administración

1. El Consejo de Administración estará integrado por un representante de cada Estado miembro y dos representantes nombrados por la Comisión. Todos los representantes tendrán derecho a voto.

2. Cada miembro del Consejo de Administración tendrá un suplente que le representará en su ausencia.

3. Los miembros del Consejo de Administración y sus suplentes serán nombrados en función de sus conocimientos en el ámbito de la ciberseguridad, teniendo en cuenta las pertinentes cualificaciones presupuestarias, administrativas y de gestión. La Comisión y los Estados miembros procurarán limitar la rotación de sus representantes en el Consejo de Administración con el fin de garantizar la continuidad en la labor de este órgano. La Comisión y los Estados miembros tratarán de alcanzar una representación equilibrada entre hombres y mujeres en el Consejo de Administración.

4. El mandato de los miembros del Consejo de Administración y de sus suplentes será de cuatro años. Este mandato será renovable.

Artículo 14
Funciones del Consejo de Administración

1. El Consejo de Administración:

   a) definirá la orientación general del funcionamiento de la Agencia y velará por que esta trabaje de conformidad con las normas y principios establecidos en el presente Reglamento; velará asimismo por la coherencia de la labor de la Agencia con las actividades realizadas por los Estados miembros y a nivel de la Unión;

   b) adoptará el proyecto de documento único de programación de la Agencia a que se refiere el artículo 21 antes de someterlo al dictamen de la Comisión;

   c) adoptará, teniendo en cuenta el dictamen de la Comisión, el documento único de programación de la Agencia por una mayoría de dos tercios de sus miembros y de conformidad con el artículo 17;

   d) adoptará, por mayoría de dos tercios de sus miembros, el presupuesto anual de la Agencia y ejercerá otras funciones relacionadas con el presupuesto de la Agencia con arreglo al capítulo III;

   e) evaluará y adoptará el informe anual consolidado sobre las actividades de la Agencia y, a más tardar el 1 de julio del año siguiente, remitirá dicho informe, junto con su evaluación, al Parlamento Europeo, al Consejo, a la

Comisión y al Tribunal de Cuentas; el informe anual incluirá las cuentas y describirá en qué medida la Agencia ha cumplido sus indicadores de rendimiento; el informe anual se hará público;

f) adoptará las normas financieras aplicables a la Agencia de conformidad con el artículo 29;

g) adoptará una estrategia contra el fraude que esté en consonancia con el riesgo de fraude, teniendo en cuenta el análisis coste-beneficio de las medidas que vayan a aplicarse;

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

i) garantizará un adecuado seguimiento de las conclusiones y recomendaciones resultantes de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF) o de las diferentes auditorías y evaluaciones, tanto internas como externas;

j) adoptará su propio reglamento interno;

k) de conformidad con el apartado 2, ejercerá, respecto del personal de la Agencia, las competencias atribuidas por el Estatuto de los funcionarios a la Autoridad facultada para proceder a los nombramientos y las atribuidas por el Régimen aplicable a los otros agentes de la Unión Europea a la Autoridad facultada para proceder a las contrataciones (en lo sucesivo, «las competencias de la Autoridad facultada para proceder a los nombramientos»);

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

m) nombrará al director ejecutivo y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 33 del presente Reglamento;

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

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

p) autorizará la celebración de convenios de trabajo de conformidad con los artículos 7 y 39.

2. El Consejo de Administración adoptará, de conformidad con el artículo 110 del Estatuto de los funcionarios, una decisión basada en el artículo 2, apartado 1, del Estatuto y en el artículo 6 del Régimen aplicable a los otros agentes, por la que se delegarán las competencias de la autoridad facultada para proceder a los nombramientos en el director ejecutivo y se definirán las condiciones en las que podrá suspenderse la delegación de competencias. El director ejecutivo estará autorizado a subdelegar esas competencias.

3. Cuando así lo exijan circunstancias excepcionales, el Consejo de Administración podrá, mediante resolución, suspender temporalmente la delegación de las competencias de la Autoridad facultada para proceder a los nombramientos en el

director ejecutivo y la subdelegación de competencias por parte de este último, y ejercer él mismo las competencias o delegarlas en uno de sus miembros o en un miembro del personal distinto del director ejecutivo.

Artículo 15
Presidente del Consejo de Administración

El Consejo de Administración elegirá entre sus miembros, por mayoría de dos tercios, a un presidente y a un vicepresidente para un período de cuatro años, que será renovable una sola vez. No obstante, si el presidente o el vicepresidente dejaran de ser miembros del Consejo de Administración durante su mandato, este expirará automáticamente en la misma fecha. El vicepresidente sustituirá de oficio al presidente cuando este no pueda desempeñar sus funciones.

Artículo 16
Reuniones del Consejo de Administración

1. Las reuniones del Consejo de Administración serán convocadas por su presidente.
2. El Consejo de Administración se reunirá al menos dos veces al año en sesión ordinaria. Celebrará también sesiones extraordinarias a instancias del presidente, de la Comisión o de como mínimo un tercio de sus miembros.
3. El director ejecutivo asistirá, sin tener derecho a voto, a las reuniones del Consejo de Administración.
4. Los miembros del Grupo Permanente de Partes Interesadas del sector podrán participar, previa invitación del presidente, en las reuniones del Consejo de Administración, sin derecho a voto.
5. Los miembros del Consejo de Administración y sus suplentes podrán estar asistidos en las reuniones por asesores o expertos, con sujeción a su reglamento interno.
6. La Agencia se encargará de la secretaría del Consejo de Administración.

Artículo 17
Votaciones en el Consejo de Administración

1. El Consejo de Administración tomará sus decisiones por mayoría de sus miembros.
2. Se requerirá una mayoría de dos tercios de todos los miembros del Consejo de Administración para aprobar el documento único de programación, el presupuesto anual y el nombramiento, prórroga del mandato o cese del director ejecutivo.
3. Cada miembro dispondrá de un voto. En ausencia de un miembro, su suplente podrá ejercer su derecho a voto.
4. El presidente participará en las votaciones.
5. El director ejecutivo no participará en las votaciones.
6. El reglamento interno del Consejo de Administración establecerá de manera más pormenorizada el régimen de votación, en particular las condiciones en las que un miembro puede actuar por cuenta de otro.

SECCIÓN 2
COMITÉ EJECUTIVO

Artículo 18
Comité Ejecutivo

1. El Consejo de Administración estará asistido por un Comité Ejecutivo.

2. El Comité Ejecutivo:

   a) preparará las resoluciones que deba adoptar el Consejo de Administración;

   b) junto con el Consejo de Administración, garantizará un seguimiento adecuado de las conclusiones y recomendaciones que se deriven de las investigaciones de la OLAF y de las distintas auditorías y evaluaciones tanto internas como externas;

   c) sin perjuicio de las responsabilidades del director ejecutivo establecidas en el artículo 19, le asistirá y asesorará en la aplicación de las decisiones del Consejo de Administración en cuestiones administrativas y presupuestarias con arreglo al artículo 19.

3. El Comité Ejecutivo estará formado por cinco miembros escogidos entre los miembros del Consejo de Administración, entre los que figurarán el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y uno de los representantes de la Comisión. El director ejecutivo participará en las reuniones del Comité Ejecutivo, pero no tendrá derecho de voto.

4. La duración del mandato de los miembros del Comité Ejecutivo será de cuatro años. Este mandato será renovable.

5. El Comité Ejecutivo se reunirá al menos una vez cada tres meses. El presidente del Comité Ejecutivo convocará otras reuniones a petición de sus miembros.

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

7. Cuando sea necesario, por motivos de urgencia, el Comité Ejecutivo podrá adoptar determinadas decisiones provisionales en nombre del Consejo de Administración, en particular en materia de gestión administrativa, incluida la suspensión de la delegación de las competencias atribuidas a la autoridad facultada para proceder a los nombramientos, y para cuestiones presupuestarias.

SECCIÓN 3
DIRECTOR EJECUTIVO

Artículo 19
Responsabilidades del director ejecutivo

1. La Agencia será gestionada por su director ejecutivo, que deberá actuar con independencia en el desempeño de sus funciones. El director ejecutivo dará cuenta de su gestión al Consejo de Administración.

2. El director ejecutivo informará al Parlamento Europeo sobre el ejercicio de sus funciones cuando se le invite a hacerlo. El Consejo podrá convocar al director ejecutivo para que le informe sobre el ejercicio de sus funciones.

3. El director ejecutivo será responsable de:

a) la administración ordinaria de la Agencia;

b) ejecutar las decisiones adoptadas por el Consejo de Administración;

c) preparar el proyecto de documento único de programación y presentarlo al Consejo de Administración para su aprobación antes de su presentación a la Comisión;

d) ejecutar el documento único de programación y presentar informes al respecto al Consejo de Administración;

e) preparar el informe anual consolidado sobre las actividades de la Agencia y presentarlo al Consejo de Administración para su evaluación y aprobación;

f) preparar un plan de acción para el seguimiento de las conclusiones de las evaluaciones retrospectivas e informar cada dos años a la Comisión sobre los progresos al respecto;

g) preparar un plan de acción sobre la base de las conclusiones de las auditorías internas o externas, así como de las investigaciones de la Oficina Europea de Lucha contra el Fraude (OLAF), y presentar informes sobre los progresos conseguidos, dos veces al año a la Comisión y regularmente al Consejo de Administración;

h) preparar el proyecto de normas financieras aplicables a la Agencia;

i) preparar el proyecto de estado de previsiones de ingresos y gastos de la Agencia y ejecutar su presupuesto;

j) proteger los intereses financieros de la Unión mediante la aplicación de medidas preventivas contra el fraude, la corrupción y cualquier otra actividad ilegal, mediante controles eficaces y, en caso de detectarse irregularidades, mediante la recuperación de los importes abonados indebidamente y, cuando proceda, mediante sanciones administrativas y financieras que sean eficaces, proporcionales y disuasorias;

k) preparar una estrategia antifraude para la Agencia y someterla a la aprobación del Consejo de Administración;

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

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

4. Siempre que sea necesario y esté dentro del mandato de la Agencia, y de conformidad con sus objetivos y tareas, el director ejecutivo podrá crear grupos de trabajo *ad hoc* integrados por expertos, incluidos expertos procedentes de las autoridades competentes de los Estados miembros. Se informará de ello anticipadamente al Consejo de Administración. Los procedimientos, en particular en

lo que se refiere a la composición de los grupos de trabajo, el nombramiento de los expertos de dichos grupos por el director ejecutivo y el funcionamiento de los grupos de trabajo, se especificarán en el reglamento operativo interno de la Agencia.

5. El director ejecutivo decidirá si es necesario ubicar a miembros de su personal en uno o más Estados miembros con el fin de desempeñar las funciones de la Agencia de manera eficiente y eficaz. Antes de tomar la decisión de establecer una oficina local, el director ejecutivo habrá de obtener el consentimiento previo de la Comisión, el Consejo de Administración y el Estado o Estados miembros de que se trate. Esta decisión especificará el alcance de las actividades que se llevarán a cabo en la oficina local, evitándose costes innecesarios y la duplicación de funciones administrativas de la Agencia. Se llegará a un acuerdo con el Estado o Estados miembros de que se trate, cuando resulte apropiado o necesario.

SECCIÓN 4
GRUPO PERMANENTE DE PARTES INTERESADAS

Artículo 20
Grupo Permanente de Partes Interesadas

1. El Consejo de Administración establecerá, a propuesta del director ejecutivo, un Grupo Permanente de Partes Interesadas integrado por expertos reconocidos que representen a las partes interesadas pertinentes, tales como la industria de las TIC, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, los grupos de consumidores, expertos académicos en ciberseguridad y representantes de las autoridades competentes notificadas con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas] y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos.

2. Los procedimientos del Grupo Permanente de Partes Interesadas, en particular con respecto al número, composición y nombramiento de sus miembros por el Consejo de Administración, a la propuesta por el director ejecutivo y al funcionamiento del Grupo, se especificarán en el reglamento operativo interno de la Agencia y se harán públicos.

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

4. El mandato de los miembros del Grupo Permanente de Partes Interesadas tendrá una duración de dos años y medio. Los miembros del Consejo de Administración no podrán ser miembros del Grupo Permanente de Partes Interesadas. Los expertos de la Comisión y de los Estados miembros podrán estar presentes en las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos Se podrá invitar a asistir a las reuniones del Grupo Permanente de Partes Interesadas y participar en sus trabajos a representantes de otros órganos que no sean miembros del mismo y el director ejecutivo considere pertinentes.

5. El Grupo Permanente de Partes Interesadas asesorará a la Agencia en lo relativo a la realización de sus actividades. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo de la Agencia y en el

mantenimiento de la comunicación con las partes interesadas pertinentes sobre todos los aspectos relativos al programa de trabajo.

SECCIÓN 5
FUNCIONAMIENTO

Artículo 21
Documento único de programación

1. La Agencia llevará a cabo sus operaciones de conformidad con un documento único de programación que contendrá su programación anual y plurianual, con inclusión de la totalidad de sus actividades previstas.

2. Cada año, el director ejecutivo elaborará un proyecto de documento único de programación que contendrá la programación anual y plurianual, con la planificación de los recursos humanos y financieros correspondientes, de conformidad con el artículo 32 del Reglamento Delegado (UE) n.º 1271/2013 de la Comisión[36] y teniendo en cuenta las directrices establecidas por la Comisión.

3. A más tardar el 30 de noviembre de cada año, el Consejo de Administración adoptará el documento único de programación a que se refiere el apartado 1 y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión a más tardar el 31 de enero del año siguiente, así como cualquier versión posterior actualizada de dicho documento.

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

5. El programa de trabajo anual incluirá objetivos detallados y los resultados esperados, incluidos indicadores de rendimiento. Contendrá asimismo una descripción de las acciones que vayan a financiarse y una indicación de los recursos humanos y financieros asignados a cada acción, de conformidad con los principios de presupuestación y gestión por actividades. El programa anual de trabajo será coherente con el programa de trabajo plurianual a que se refiere el apartado 7. Indicará claramente qué tareas se han añadido, modificado o suprimido en relación con el ejercicio presupuestario anterior.

6. El Consejo de Administración modificará el programa de trabajo anual adoptado cuando se encomiende una nueva tarea a la Agencia. Cualquier modificación sustancial del programa de trabajo anual se adoptará con arreglo al mismo procedimiento que el programa de trabajo anual inicial. El Consejo de Administración podrá delegar en el director ejecutivo la facultad de adoptar modificaciones no sustanciales del programa de trabajo anual.

7. El programa de trabajo plurianual fijará la programación estratégica general, incluidos los objetivos, los resultados esperados y los indicadores de rendimiento.

---

36 Reglamento Delegado (UE) n.º 1271/2013 de la Comisión, de 30 de septiembre de 2013, relativo al Reglamento financiero marco de los organismos a que se refiere el artículo 208 del Reglamento (UE, Euratom) n.º 966/2012 del Parlamento Europeo y del Consejo (DO L 328 de 7.12.2013, p. 42).

Definirá asimismo la programación de los recursos, incluidos el presupuesto plurianual y el personal.

8. La programación de los recursos se actualizará todos los años. La programación estratégica se actualizará cuando proceda, y en particular cuando resulte necesario a la luz de los resultados de la evaluación a que se refiere el artículo 56.

Artículo 22
Declaración de intereses

1. Los miembros del Consejo de Administración, el director ejecutivo y los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal deberán efectuar cada uno de ellos una declaración de compromisos y otra declaración en la que indiquen si tienen o no intereses directos o indirectos que pudieran considerarse perjudiciales para su independencia. Las declaraciones serán exactas y completas, se presentarán anualmente por escrito y se actualizarán siempre que sea necesario.

2. Los miembros del Consejo de Administración, el director ejecutivo y los expertos externos que participen en los grupos de trabajo *ad hoc* deberán declarar cada uno de ellos de forma exacta y completa, a más tardar al comienzo de cada reunión, cualquier interés que pudiera considerarse perjudicial para su independencia en relación con los puntos del orden del día y deberán abstenerse de participar en los debates y en la votación sobre esos puntos.

3. La Agencia establecerá en su reglamento operativo interno las medidas prácticas correspondientes a las normas sobre declaraciones de intereses a que se refieren los apartados 1 y 2.

Artículo 23
Transparencia

1. La Agencia llevará a cabo sus actividades con un alto grado de transparencia y de conformidad con el artículo 25.

2. La Agencia velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 22.

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

4. La Agencia establecerá en su reglamento operativo interno las medidas prácticas de aplicación de las normas de transparencia a que se refieren los apartados 1 y 2.

Artículo 24
Confidencialidad

1. Sin perjuicio de lo dispuesto en el artículo 25, la Agencia no divulgará a terceros la información que procese o reciba para la que se haya presentado una solicitud motivada de tratamiento confidencial referida a todo la información o a parte de ella.

2. Los miembros del Consejo de Administración, el director ejecutivo, los miembros del Grupo Permanente de Partes Interesadas, los expertos externos que participen en los grupos de trabajo *ad hoc* y los miembros del personal de la Agencia, incluidos los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal, respetarán la obligación de confidencialidad en virtud del artículo 339 del Tratado de Funcionamiento de la Unión Europea (TFUE), incluso después de haber cesado en sus cargos.

3. La Agencia establecerá en su reglamento operativo interno las medidas prácticas de aplicación de las normas de confidencialidad a que se refieren los apartados 1 y 2.

4. Si así lo exige el desempeño de los cometidos de la Agencia, el Consejo de Administración tomará la decisión de permitir a la Agencia manejar información clasificada. En tal caso, el Consejo de Administración, de común acuerdo con los servicios de la Comisión, adoptará un reglamento operativo interno que aplique los principios de seguridad contenidos en las Decisiones (UE, Euratom) 2015/443[37] y 2015/444[38] de la Comisión. Dicho reglamento incluirá, entre otras, disposiciones para el intercambio, tratamiento y almacenamiento de la información clasificada.

Artículo 25
Acceso a los documentos

1. Se aplicará a los documentos en poder de la Agencia el Reglamento (CE) n.º 1049/2001.

2. El Consejo de Administración adoptará disposiciones para la aplicación del Reglamento (CE) n.º 1049/2001 en el plazo de seis meses a partir del establecimiento de la Agencia.

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

CAPÍTULO III
ESTABLECIMIENTO Y ESTRUCTURA DEL PRESUPUESTO

Artículo 26
Establecimiento del presupuesto

1. El director ejecutivo elaborará cada año un proyecto de declaración sobre la previsión de los ingresos y los gastos de la Agencia para el siguiente ejercicio financiero, y lo hará llegar al Consejo de Administración, junto con un proyecto de plantilla. Los ingresos y los gastos deberán estar equilibrados.

[37] Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (DO L 72 de 17.3.2015, p. 41).

[38] Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

2. El Consejo de Administración presentará cada año, sobre la base del proyecto de previsión de ingresos y gastos a que se refiere el apartado 1, la previsión de ingresos y gastos de la Agencia para el siguiente ejercicio financiero.

3. El Consejo de Administración, a más tardar el 31 de enero de cada año, transmitirá la previsión a que se refiere el apartado 2, que formará parte del proyecto de documento único de programación, a la Comisión y a los terceros países con los que la Unión haya celebrado acuerdos de conformidad con el artículo 39.

4. Sobre la base de dicha previsión, la Comisión consignará en el proyecto de presupuesto general de la Unión Europea las previsiones que considere necesarias para la plantilla y el importe de la contribución que se imputará al presupuesto general, que deberá presentar al Parlamento Europeo y al Consejo de conformidad con los artículos 313 y 314 del TFUE.

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

6. El Parlamento Europeo y el Consejo aprobarán la plantilla de la Agencia.

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

Artículo 27
Estructura del presupuesto

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

   a) una contribución procedente del presupuesto de la Unión;

   b) ingresos asignados a partidas de gastos específicas de conformidad con sus normas financieras mencionadas en el artículo 29;

   c) financiación de la Unión en forma de convenios de delegación o subvenciones *ad hoc*, de conformidad con sus normas financieras mencionadas en el artículo 29 y las disposiciones de los instrumentos pertinentes de apoyo a las políticas de la Unión;

   d) contribuciones de terceros países que participen en los trabajos de la Agencia tal como prevé el artículo 39;

   e) eventuales contribuciones voluntarias de los Estados miembros en efectivo o en especie; los Estados miembros que aporten contribuciones voluntarias no podrán reclamar ningún derecho o servicio específico como consecuencia de su contribución.

2. Los gastos de la Agencia incluirán los gastos de personal, administrativos y de soporte técnico, de infraestructura y funcionamiento, así como los gastos derivados de contratos suscritos con terceros.

Artículo 28

Ejecución del presupuesto

1. El director ejecutivo será responsable de la ejecución del presupuesto de la Agencia.
2. El auditor interno de la Comisión ejercerá, con respecto a la Agencia, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión.
3. A más tardar el 1 de marzo siguiente a un ejercicio financiero (1 de marzo del año N+1), el contable de la Agencia remitirá las cuentas provisionales al contable de la Comisión y al Tribunal de Cuentas.
4. Tras recibir las observaciones formuladas por el Tribunal de Cuentas sobre las cuentas provisionales de la Agencia, el contable de esta elaborará las cuentas definitivas de la Agencia bajo su responsabilidad.
5. El director ejecutivo presentará las cuentas definitivas al Consejo de Administración para que este emita dictamen al respecto.
6. A más tardar el 31 de marzo del año N + 1, el director ejecutivo remitirá el informe sobre la gestión presupuestaria y financiera al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas.
7. A más tardar el 1 de julio del año N + 1, el contable remitirá las cuentas definitivas, juntamente con el dictamen del Consejo de Administración, al Parlamento Europeo, al Consejo, al contable de la Comisión y al Tribunal de Cuentas.
8. En la misma fecha de transmisión de sus cuentas definitivas, el contable también enviará al Tribunal de Cuentas una toma de posición relativa a estas cuentas definitivas, con copia al contable de la Comisión.
9. El director ejecutivo publicará las cuentas definitivas a más tardar el 15 de noviembre del año siguiente.
10. El director ejecutivo remitirá al Tribunal de Cuentas una respuesta a sus observaciones a más tardar el 30 de septiembre del año N + 1, y enviará asimismo copia de dicha respuesta al Consejo de Administración y a la Comisión.
11. El director ejecutivo presentará al Parlamento Europeo, cuando este lo solicite, toda la información necesaria para el correcto desarrollo del procedimiento de aprobación de la ejecución del presupuesto del ejercicio de que se trate, según se establece en el artículo 165, apartado 3, del Reglamento Financiero.
12. El Parlamento Europeo, sobre la base de una recomendación del Consejo, deberá aprobar la gestión del director ejecutivo antes del 15 de mayo del año N + 2 respecto a la ejecución del presupuesto del año N.

Artículo 29

Normas financieras

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

Artículo 30
Lucha contra el fraude

1. Con el fin de facilitar la lucha contra el fraude, la corrupción y otras actividades ilegales con arreglo al Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo[39], la Agencia, en el plazo de seis meses a partir de la fecha en que comience a operar, suscribirá el Acuerdo Interinstitucional, de 25 de mayo de 1999, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF), y adoptará las disposiciones pertinentes, que serán de aplicación a todo el personal de la Agencia, sirviéndose del modelo contenido en el anexo de dicho Acuerdo.

2. El Tribunal de Cuentas tendrá la facultad de auditar, sobre la base de documentos y sobre el terreno, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido de la Agencia fondos de la Unión.

3. La OLAF podrá realizar investigaciones, incluidos controles y verificaciones sobre el terreno, de conformidad con las disposiciones y los procedimientos establecidos en el Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo y el Reglamento (Euratom, CE) n.º 2185/96 del Consejo[40], de 11 de noviembre de 1996, relativo a los controles y verificaciones *in situ* que realiza la Comisión para la protección de los intereses financieros de las Comunidades Europeas contra los fraudes e irregularidades, con el fin de determinar si ha habido fraude, corrupción o cualquier otra actividad ilegal que afecte a los intereses financieros de la Unión en relación con una subvención o un contrato financiado por la Agencia.

4. Sin perjuicio de lo dispuesto en los apartados 1, 2 y 3, los acuerdos de cooperación con terceros países y con organizaciones internacionales, así como los contratos y los convenios y decisiones de subvención de la Agencia, contendrán disposiciones que establezcan expresamente la potestad del Tribunal de Cuentas y de la OLAF de llevar a cabo las auditorías y las investigaciones mencionadas, según sus respectivas competencias.

CAPÍTULO IV
PERSONAL DE LA AGENCIA

Artículo 31
Disposiciones generales

Se aplicarán al personal de la Agencia el Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, así como las normas adoptadas por acuerdo entre las instituciones de la Unión con el fin de poner en práctica tales disposiciones.

---

39 Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) y por el que se deroga el Reglamento (CE) n.º 1073/1999 del Parlamento Europeo y del Consejo y el Reglamento (Euratom) n.º 1074/1999 del Consejo (DO L 248 de 18.9.2013, p. 1).

40 Reglamento (Euratom, CE) n.º 2185/96 del Consejo, de 11 de noviembre de 1996, relativo a los controles y verificaciones *in situ* que realiza la Comisión para la protección de los intereses financieros de las Comunidades Europeas contra los fraudes e irregularidades (DO L 292 de 15.11.1996, p. 2).

Artículo 32

Privilegios e inmunidades

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

Artículo 33

Director ejecutivo

1. El director ejecutivo será contratado como agente temporal de la Agencia según lo dispuesto en el artículo 2, letra a), del Régimen aplicable a los otros agentes.
2. El director ejecutivo será nombrado por el Consejo de Administración a partir de una lista de candidatos propuesta por la Comisión en el marco de un procedimiento de selección abierto y transparente.
3. Para la celebración del contrato del director ejecutivo, la Agencia estará representada por el presidente del Consejo de Administración.
4. Antes del nombramiento, se invitará al candidato seleccionado por el Consejo de Administración a hacer una declaración ante la comisión pertinente del Parlamento Europeo y a responder a las preguntas formuladas por los parlamentarios.
5. El mandato del director ejecutivo tendrá una duración de cinco años. Al final de ese período, la Comisión realizará una evaluación en la que se analizarán la actuación del director ejecutivo y las futuras tareas y desafíos de la Agencia.
6. El Consejo de Administración se pronunciará sobre el nombramiento, la prórroga del mandato o el cese del director ejecutivo por mayoría de dos tercios de sus miembros con derecho de voto.
7. A propuesta de la Comisión, en la que se tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá prorrogar una vez el mandato del director ejecutivo, por un plazo máximo de cinco años.
8. El Consejo de Administración informará al Parlamento Europeo acerca de su intención de prorrogar el mandato del director ejecutivo. En los tres meses que precedan a la prórroga de su mandato, el director ejecutivo hará, si se le invita a ello, una declaración ante la comisión pertinente del Parlamento Europeo y responderá a las preguntas formuladas por los parlamentarios.
9. Un director ejecutivo cuyo mandato haya sido prorrogado no podrá participar en otro procedimiento de selección para el mismo puesto.
10. El director ejecutivo solo podrá ser cesado por una decisión del Consejo de Administración, a propuesta de la Comisión.

Artículo 34

Expertos nacionales en comisión de servicios y otros agentes

1. La Agencia podrá recurrir a expertos nacionales en comisión de servicios o a otro personal no contratado por la Agencia. El Estatuto de los funcionarios y el Régimen aplicable a los otros agentes no serán de aplicación a este personal.
2. El Consejo de Administración adoptará una decisión que establezca las normas aplicables a las comisiones de servicios de expertos nacionales en la Agencia.

CAPÍTULO V
DISPOSICIONES GENERALES

Artículo 35
Estatuto jurídico de la Agencia

1. La Agencia será un órgano de la Unión dotado de personalidad jurídica.
2. En cada Estado miembro, la Agencia disfrutará de la capacidad jurídica más amplia que se conceda a las personas jurídicas en el Derecho interno. En particular, podrá adquirir o vender propiedad mobiliaria e inmobiliaria y ser parte en actuaciones judiciales.
3. La Agencia estará representada por su director ejecutivo.

Artículo 36
Responsabilidad de la Agencia

1. La responsabilidad contractual de la Agencia se regirá por la legislación aplicable al contrato de que se trate.
2. El Tribunal de Justicia de la Unión Europea será competente para pronunciarse en virtud de cualquier cláusula arbitral contenida en un contrato firmado por la Agencia.
3. En materia de responsabilidad extracontractual, la Agencia deberá reparar los daños causados por ella o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a las legislaciones de los Estados miembros.
4. El Tribunal de Justicia de la Unión Europea será competente para conocer de todos los litigios relativos a la indemnización por esos daños.
5. La responsabilidad personal de los agentes respecto a la Agencia se regirá por las disposiciones pertinentes aplicables al personal de la Agencia.

Artículo 37
Régimen lingüístico

1. Se aplicarán a la Agencia las disposiciones establecidas en el Reglamento n.º 1[41]. Los Estados miembros y los demás organismos nombrados por ellos podrán dirigirse a la Agencia y obtener respuesta en la lengua oficial de las instituciones de la Unión Europea que elijan.
2. Los servicios de traducción requeridos para el funcionamiento de la Agencia serán prestados por el Centro de Traducción de los Órganos de la Unión Europea.

[41] Reglamento nº 1 por el que se fija el régimen lingüístico de la Comunidad Europea de la Energía Atómica (DO 17 de 6.10.1958, p. 401).

Artículo 38

Protección de los datos personales

1. El tratamiento de los datos personales por parte de la Agencia deberá ajustarse al Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[42].

2. El Consejo de Administración adoptará las normas complementarias a que se refiere el artículo 24, apartado 8, del Reglamento (CE) n.º 45/2001. El Consejo de Administración podrá adoptar otras medidas necesarias para la aplicación del Reglamento (CE) n.º 45/2001 por parte de la Agencia.

Artículo 39

Cooperación con terceros países y organizaciones internacionales

1. En la medida en que resulte necesario para el logro de los objetivos fijados en el presente Reglamento, la Agencia podrá cooperar con las autoridades competentes de terceros países, con organizaciones internacionales, o con ambas. Para ello, la Agencia podrá, previa aprobación de la Comisión, establecer acuerdos de trabajo con las autoridades de terceros países y organizaciones internacionales. Dichos acuerdos no impondrán obligaciones jurídicas que incumban a la Unión y sus Estados miembros.

2. La Agencia estará abierta a la participación de terceros países que hayan celebrado acuerdos con la Unión en este sentido. Con arreglo a las disposiciones pertinentes de dichos acuerdos, se irán estableciendo mecanismos que precisen, en particular, el carácter, el alcance y las modalidades de participación de cada uno de estos países en la labor de la Agencia, incluidas disposiciones sobre la participación en las iniciativas emprendidas por la Agencia, las contribuciones financieras y el personal. Por lo que se refiere al personal, dichos mecanismos serán, en cualquier caso, conformes con el Estatuto de los funcionarios.

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

Artículo 40

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

La Agencia, en consulta con la Comisión, adoptará sus normas de seguridad aplicando los principios de seguridad contenidos en las normas de seguridad de la Comisión para la protección de la información clasificada de la Unión Europea (ICUE) y la información sensible no clasificada, según lo dispuesto en las Decisiones (UE, Euratom) 2015/443 y 2015/444. Esto incluirá, entre otras cosas, disposiciones para el intercambio, tratamiento y almacenamiento de este tipo de información.

---

42 Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

Artículo 41

Acuerdo relativo a la sede y condiciones de funcionamiento

1. Las disposiciones necesarias relativas a la instalación que se habilitará para la Agencia en el Estado miembro de acogida y los recursos que debe poner a su disposición dicho Estado miembro, así como las normas específicas aplicables en el Estado miembro de acogida al director ejecutivo, a los miembros del Consejo de Administración, al personal de la Agencia y a los miembros de sus familias se fijarán en un acuerdo de sede celebrado entre la Agencia y el Estado miembro de acogida concluido, previa aprobación del Consejo de Administración, a más tardar [dos años después de la entrada en vigor del presente Reglamento].

2. El Estado miembro que acoja a la Agencia ofrecerá las mejores condiciones posibles para garantizar su buen funcionamiento, incluida la accesibilidad de su ubicación, la presencia de servicios educativos adecuados para los hijos de los miembros del personal y un acceso adecuado al mercado de trabajo, la seguridad social y la atención médica para hijos y cónyuges.

Artículo 42

Control administrativo

El funcionamiento de la Agencia será supervisado por el Defensor del Pueblo Europeo de conformidad con el artículo 228 del TFUE.

TÍTULO III
MARCO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD

Artículo 43

Regímenes europeos de certificación de la ciberseguridad

Un régimen europeo de certificación de la ciberseguridad confirmará que los productos y servicios de TIC que hayan sido certificados con arreglo a dicho régimen cumplen los requisitos especificados en lo que respecta a su capacidad para resistir, con un determinado nivel de garantía, las acciones encaminadas a poner en peligro la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, estos productos, procesos, servicios y sistemas.

Artículo 44

Preparación y adopción de un régimen europeo de certificación de la ciberseguridad

1. Tras recibir una solicitud de la Comisión, ENISA preparará una propuesta de régimen europeo de certificación de la ciberseguridad que cumpla los requisitos expuestos en los artículos 45, 46 y 47 del presente Reglamento. Los Estados miembros o el Grupo Europeo de Certificación de la Ciberseguridad («el Grupo») establecido de conformidad con el artículo 53 podrán proponer a la Comisión la preparación de un régimen europeo de certificación de la ciberseguridad.
2. A la hora de preparar las propuestas de régimen a que se refiere el apartado 1 del presente artículo, ENISA consultará a todas las partes interesadas y cooperará estrechamente con el Grupo. El Grupo facilitará a ENISA la asistencia y el asesoramiento experto que requiera en relación con la preparación de la propuesta de régimen, incluso mediante la emisión de dictámenes en caso necesario.
3. ENISA transmitirá a la Comisión la propuesta de régimen europeo de certificación de la ciberseguridad preparada de conformidad con el apartado 2 del presente artículo.
4. La Comisión, sobre la base de la propuesta de régimen preparada por ENISA, podrá adoptar actos de ejecución, de conformidad con el artículo 55, apartado 1, que establezcan regímenes europeos de certificación de la ciberseguridad para productos y servicios de TIC que cumplan los requisitos de los artículos 45, 46 y 47 del presente Reglamento.
5. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los regímenes europeos de certificación de la ciberseguridad y darles publicidad.

Artículo 45

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

Los regímenes europeos de certificación de la ciberseguridad deberán diseñarse para tener en cuenta, según proceda, los siguientes objetivos de seguridad:

a) proteger los datos almacenados, transmitidos o procesados de otro modo frente al almacenamiento, procesamiento, acceso o revelación accidentales o no autorizados;

b) proteger los datos almacenados, transmitidos o procesados de otro modo frente a la destrucción accidental o no autorizada, la pérdida accidental o la alteración;

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

d) registrar qué datos, funciones o servicios se han comunicado, en qué momentos y por quién;

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

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

g) garantizar que los productos y servicios de TIC se entreguen siempre con un *software* actualizado, que no contenga vulnerabilidades conocidas, y dispongan de mecanismos para efectuar actualizaciones de seguridad del *software*.

Artículo 46

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

1. Un régimen europeo de certificación de la ciberseguridad podrá especificar uno o más de los siguientes niveles de garantía: básico, sustancial y/o elevado, para los productos y servicios de TIC amparados en dicho régimen.

2. Los niveles de garantía básico, sustancial y elevado cumplirán los siguientes criterios, respectivamente:

a) el nivel de garantía bajo se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado limitado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir el riesgo de incidentes de ciberseguridad;

b) el nivel de garantía sustancial se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado sustancial de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC, y se caracteriza en referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objeto es reducir sustancialmente el riesgo de incidentes de ciberseguridad;

c) el nivel de garantía elevado se referirá a un certificado, expedido en el contexto de un régimen europeo de certificación de la ciberseguridad, que aporta un grado de confianza en las cualidades de ciberseguridad pretendidas o declaradas de un producto o servicio de TIC superior al de los certificados con nivel de garantía sustancial, y se caracteriza en referencia a especificaciones

técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es evitar los incidentes de ciberseguridad.

Artículo 47

Elementos de los regímenes europeos de certificación de la ciberseguridad

1. Un régimen europeo de certificación de la ciberseguridad incluirá los siguientes elementos:

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

   b) especificación detallada de los requisitos de ciberseguridad con respecto a los cuales se evalúan los servicios y productos de TIC, por ejemplo haciendo referencia a normas o especificaciones técnicas internacionales o de la Unión;

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

   d) criterios y métodos específicos de evaluación, incluidos los tipos de evaluación, para demostrar el logro de los objetivos específicos a que se refiere el artículo 45;

   e) información necesaria para la certificación que deben facilitar los solicitantes a los organismos de evaluación de la conformidad;

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

   g) cuando la vigilancia forme parte del régimen, las normas para controlar el cumplimiento de los requisitos de los certificados, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

   h) condiciones para la concesión, el mantenimiento, la continuación, la ampliación y la reducción del alcance de la certificación;

   i) normas relativas a las consecuencias de la no conformidad de los productos y servicios de TIC certificados con los requisitos de certificación;

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

   k) normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad;

   l) identificación de los regímenes nacionales de certificación de la ciberseguridad que cubren el mismo tipo o categoría de productos y servicios de TIC;

   m) contenido del certificado expedido.

2. Los requisitos del régimen especificados no podrán contravenir ningún requisito legal aplicable, en particular los que emanen de la legislación armonizada de la Unión.

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

4. En ausencia de legislación armonizada de la Unión, la legislación de los Estados miembros podrá prever también el uso de un régimen europeo de certificación de la ciberseguridad para establecer la presunción de conformidad con los requisitos legales.

Artículo 48

Certificación de la ciberseguridad

1. Los productos y servicios de TIC que hayan sido certificados de conformidad con un régimen europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 44 se presumirán conformes con los requisitos de dicho régimen.

2. La certificación será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión.

3. Los organismos de evaluación de la conformidad a que se refiere el artículo 51 expedirán un certificado europeo de ciberseguridad en virtud del presente artículo sobre la base de los criterios incluidos en el régimen europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 44.

4. No obstante lo dispuesto en el apartado 3, en casos debidamente justificados un régimen europeo de ciberseguridad particular podrá prever que solo un organismo público pueda expedir un certificado europeo de ciberseguridad resultante de ese régimen. Este organismo público será uno de los siguientes:

   a) una autoridad nacional de supervisión de la certificación con arreglo al artículo 50, apartado 1;

   b) un organismo que esté acreditado como organismo de evaluación de la conformidad con arreglo al artículo 51, apartado 1; o

   c) un organismo establecido con arreglo a las leyes, instrumentos jurídicos u otros procedimientos administrativos oficiales del Estado miembro de que se trate y que cumple los requisitos para los organismos que certifican productos, procesos y servicios con arreglo a la norma ISO/IEC 17065:2012.

5. La persona física o jurídica que presenta sus productos o servicios de TIC al mecanismo de certificación facilitará al organismo de evaluación de la conformidad a que se refiere el artículo 51 toda la información necesaria para llevar a cabo el procedimiento de certificación.

6. Los certificados se expedirán por un período máximo de tres años y podrán renovarse en las mismas condiciones, siempre y cuando sigan cumpliéndose los requisitos correspondientes.

7. Los certificados europeos de ciberseguridad expedidos de conformidad con el presente artículo serán reconocidos en todos los Estados miembros.

Artículo 49

Regímenes y certificados nacionales de certificación de la ciberseguridad

1. Sin perjuicio de lo dispuesto en el apartado 3, los regímenes nacionales de certificación de ciberseguridad y los procedimientos correspondientes para los productos y servicios de TIC cubiertos por un régimen 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 44, apartado 4. Los regímenes nacionales de certificación de la ciberseguridad existentes y los procedimientos conexos para los productos y servicios de TIC no cubiertos por un régimen europeo de certificación de la ciberseguridad seguirán existiendo.

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

3. Los certificados existentes expedidos de conformidad con regímenes nacionales de certificación de ciberseguridad seguirán siendo válidos hasta su fecha de caducidad.

Artículo 50

Autoridades nacionales de supervisión de la certificación

1. Cada Estado miembro designará una autoridad nacional de supervisión de la certificación.

2. Cada Estado miembro informará a la Comisión de la identidad de la autoridad designada.

3. Las autoridades nacionales de supervisión de la certificación serán, en lo relativo a su organización, sus decisiones de financiación, su estructura jurídica y su proceso de toma de decisiones, independientes de las entidades que están bajo su supervisión.

4. Los Estados miembros velarán por que las autoridades nacionales de supervisión de la certificación dispongan de los recursos adecuados para ejercer sus competencias y llevar a cabo, de manera eficaz y eficiente, las tareas que tienen encomendadas.

5. Para la aplicación eficaz del Reglamento, es conveniente que estas autoridades participen en el Grupo Europeo de Certificación de la Ciberseguridad establecido con arreglo al artículo 53 de manera activa, eficaz, eficiente y segura.

6. Las autoridades nacionales de supervisión de la certificación:

   a) controlarán e impondrán la aplicación de las disposiciones del presente título a nivel nacional y supervisarán la conformidad de los certificados que hayan sido emitidos por los organismos de evaluación de la conformidad establecidos en sus territorios respectivos con los requisitos establecidos en el presente título y en el correspondiente régimen europeo de certificación de la ciberseguridad;

   b) controlarán y supervisarán las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento, en particular en relación con la notificación de los organismos de evaluación de la conformidad y las tareas conexas establecidas en el artículo 52 del presente Reglamento;

   c) tramitarán las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados expedidos por los organismos de evaluación de la conformidad establecidos en su territorio, investigarán el asunto objeto de la reclamación en la medida que proceda e informarán al reclamante sobre el curso y el resultado de la investigación en un plazo razonable;

   d) cooperarán con otras autoridades nacionales de supervisión de la certificación u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos y servicios de TIC que no se ajusten a los

requisitos del presente Reglamento o de regímenes europeos de ciberseguridad específicos;

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

7. Cada autoridad nacional de supervisión de la certificación tendrá, como mínimo, las siguientes competencias:

a) solicitar a los organismos de evaluación de la conformidad y a los titulares de certificados europeos de ciberseguridad que faciliten cualquier información que requiera para el desempeño de sus cometidos;

b) llevar a cabo investigaciones, en forma de auditorías, de los organismos de evaluación de la conformidad y los titulares de certificados europeos de ciberseguridad, a efectos de verificar el cumplimiento de lo dispuesto en el título III;

c) adoptar las medidas adecuadas, de conformidad con el Derecho nacional, con el fin de garantizar que los organismos de evaluación de la conformidad o los titulares de certificados se ajustan al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad;

d) obtener acceso a todos los locales de los organismos de evaluación de la conformidad y los titulares de certificados europeos de ciberseguridad para la realización de investigaciones con arreglo al Derecho de la Unión o al Derecho procesal del Estado miembro;

e) retirar, con arreglo al Derecho nacional, los certificados que no se ajusten al presente Reglamento o a un régimen europeo de certificación de la ciberseguridad;

f) imponer sanciones, según lo previsto en el artículo 54, con arreglo al Derecho nacional, y solicitar el cese inmediato de la violación de las obligaciones establecidas en el presente Reglamento.

8. Las autoridades nacionales de supervisión de la certificación 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 y servicios de TIC.

Artículo 51

Organismos de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad estarán acreditados por el organismo nacional de acreditación designado con arreglo al Reglamento (CE) n.º 765/2008 solamente si cumplen los requisitos establecidos en el anexo del presente Reglamento.

2. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos establecidos en el presente artículo. Los organismos de acreditación revocarán la acreditación de un organismo de evaluación de la conformidad concedida en virtud del apartado 1 del presente artículo cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la

actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

Artículo 52
Notificación

1. En relación con cada régimen europeo de certificación de la ciberseguridad adoptado con arreglo al artículo 44, las autoridades nacionales de supervisión de la certificación notificarán a la Comisión los correspondientes organismos de evaluación de la conformidad acreditados para expedir certificados de los niveles de garantía especificados en el artículo 46 y, sin dilaciones indebidas, cualquier modificación al respecto.
2. Un año después de la entrada en vigor de un régimen europeo de certificación de la ciberseguridad, la Comisión publicará en el Diario Oficial una lista de los organismos de evaluación de la conformidad notificados.
3. Si la Comisión recibe una notificación una vez concluido el período a que se refiere el apartado 2, publicará en el Diario Oficial de la Unión Europea las modificaciones de la lista a que se refiere el apartado 2 en el plazo de dos meses a partir de la fecha de recepción de dicha notificación.
4. Una autoridad nacional de supervisión de la certificación podrá presentar a la Comisión una solicitud para retirar de la lista a la que se refiere el apartado 2 del presente artículo a un organismo de evaluación de la conformidad notificado por dicha autoridad nacional de supervisión de la certificación. La Comisión publicará en el Diario Oficial de la Unión Europea las modificaciones correspondientes de la lista en el plazo de un mes a partir de la fecha de recepción de la solicitud de la autoridad nacional de supervisión de la certificación.
5. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos de las notificaciones a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 55, apartado 2.

Artículo 53
Grupo Europeo de Certificación de la Ciberseguridad

1. Queda establecido el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «el Grupo»).
2. El Grupo estará integrado por las autoridades nacionales de supervisión de la certificación. Las autoridades estarán representadas por los directores u otros representantes de alto nivel de las autoridades nacionales de supervisión de la certificación.
3. El Grupo desempeñará las siguientes tareas:
   a) asesorar y asistir a la Comisión en su labor de garantizar la coherencia en la implantación y aplicación del presente título, en particular en relación con las cuestiones de política de certificación de la ciberseguridad, la coordinación de los enfoques políticos y la preparación de los regímenes europeos de certificación de la ciberseguridad;

b) asistir, asesorar y cooperar con ENISA en relación con la preparación de una propuesta de régimen, de conformidad con el artículo 44 del presente Reglamento;

c) proponer a la Comisión que solicite a la Agencia que prepare una propuesta de régimen europeo de certificación de la ciberseguridad de conformidad con el artículo 44 del presente Reglamento;

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

e) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar buenas prácticas sobre los regímenes de certificación de la ciberseguridad;

f) facilitar la cooperación entre las autoridades nacionales de supervisión de la certificación en virtud del presente título mediante el intercambio de información, y en particular mediante el establecimiento de métodos para un intercambio de información eficaz en relación con todos los temas relacionados con la certificación de la ciberseguridad.

4. La Comisión presidirá el Grupo y se hará cargo de su secretaría, con la asistencia de ENISA según lo previsto en el artículo 8, letra a).

Artículo 54
Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables a los incumplimientos del presente título y de los regímenes europeos de certificación de la ciberseguridad y adoptarán toda medida necesaria para garantizar su aplicación. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias. Los Estados miembros notificarán a la Comisión [a más tardar el …/sin demora] dicho régimen y dichas medidas, así como cualquier modificación posterior que les afecte.

TÍTULO IV
DISPOSICIONES FINALES

Artículo 55
Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento (UE) n.º 182/2011.

Artículo 56
Evaluación y revisión

1. A más tardar cinco años después de la fecha a que se refiere el artículo 58, y posteriormente cada cinco años, la Comisión evaluará el impacto, la eficacia y la eficiencia de la Agencia 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 la Agencia en respuesta a sus actividades. Si la Comisión considerara que la continuidad de la Agencia ha dejado de estar justificada con respecto a los objetivos, mandato y tareas que le fueron atribuidos, podrá proponer que se modifique el presente Reglamento en lo que se refiere a las disposiciones relacionadas con la Agencia.

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

3. La Comisión remitirá el informe de evaluación, conjuntamente con sus conclusiones, al Parlamento Europeo, al Consejo y al Consejo de Administración. Los resultados de dicho informe se harán públicos.

Artículo 57
Derogación y sucesión

1. Queda derogado el Reglamento (CE) n.º 526/2013, con efecto desde el [….].

2. Las referencias al Reglamento (CE) n.º 526/2013 y a ENISA se entenderán hechas al presente Reglamento y a la Agencia.

3. La Agencia será considerada sucesora de la establecida por el Reglamento (CE) n.º 526/2013 en todo lo que se refiere a propiedad, acuerdos, obligaciones legales, contratos de empleo, compromisos financieros y responsabilidades. Todas las decisiones existentes del Consejo de Administración y del Comité Ejecutivo seguirán

siendo válidas, a condición de que no sean incompatibles con las disposiciones del presente Reglamento.

4. La Agencia se establece por un período indefinido a partir del [….].

5. El director ejecutivo nombrado de conformidad con el artículo 24, apartado 4, del Reglamento (CE) n.º 526/2013 será el director ejecutivo de la Agencia para el resto de su mandato.

6. Los miembros del Consejo de Administración designados de conformidad con el artículo 6 del Reglamento (CE) n.º 526/2013 y sus suplentes serán los miembros y sus suplentes del Consejo de Administración de la Agencia para el resto de su mandato.

Artículo 58

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

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

Hecho en Bruselas, el

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

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la «Agencia de Ciberseguridad de la UE»), y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad en las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

1.2. Ámbito(s) político(s) afectado(s)

Ámbito político: 09 - Redes de comunicaciones, contenidos y tecnología

Actividad: 09.02 - Mercado único digital

1.3. Naturaleza de la propuesta/iniciativa

☒ La propuesta/iniciativa se refiere a **una acción nueva (título III – Certificación)**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[43]

☒La propuesta/iniciativa se refiere a **la prolongación de una acción existente** (**título II – mandato de ENISA)**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa

1. Aumentar la resiliencia de los Estados miembros, las empresas y el conjunto de la UE

2. Garantizar el buen funcionamiento del mercado interior de productos y servicios de TIC de la UE

3. Aumentar la competitividad global de las empresas de la UE que operan en el ámbito de las TIC.

4. Aproximar las disposiciones legales, reglamentarias y administrativas de los Estados miembros que exijan ciberseguridad.

1.4.2. Objetivo(s) específico(s)

Teniendo en mente los objetivos generales, en el contexto más amplio de la revisión de la Estrategia de Ciberseguridad, el instrumento, delimitando el ámbito de actuación y el mandato de ENISA y estableciendo el marco europeo para la certificación de productos y servicios de TIC, se propone alcanzar los siguientes objetivos específicos:

1. Aumentar **las capacidades y la preparación** de los Estados miembros y de las empresas.
2. Mejorar **la cooperación y la coordinación** entre los Estados miembros y las instituciones, órganos y organismos de la UE.
3. Aumentar **las capacidades a nivel de la UE para complementar la acción de los**

[43] Tal como se contempla en el artículo 54, apartado 2, letras a) o b), del Reglamento Financiero.

Estados miembros, en particular en caso de cibercrisis transfronteriza.

4. Aumentar **la sensibilización** de ciudadanos y empresas sobre las cuestiones relacionadas con la ciberseguridad.
5. Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la **transparencia global de la garantía de ciberseguridad**[44] de los productos y servicios de TIC.

ENISA contribuirá a la consecución de los citados objetivos mediante:

La mejora del apoyo a la formulación de políticas: Facilitar orientaciones y asesoramiento a la Comisión y a los Estados miembros para actualizar y desarrollar un marco normativo holístico en el ámbito de la ciberseguridad, así como políticas sectoriales e iniciativas legales cuando estén presentes cuestiones relacionadas con la ciberseguridad; contribuir a los trabajos del Grupo de cooperación (artículo 11 de la Directiva (UE) 2016/1148), ofreciendo asesoramiento y asistencia; apoyar el desarrollo y la aplicación de políticas en el ámbito de la identidad electrónica y los servicios de confianza; promover el intercambio de las mejores prácticas entre las autoridades competentes.

La mejora del apoyo a la creación de capacidades: Prestar apoyo a los Estados miembros y a las instituciones, órganos y organismos de la Unión para desarrollar y mejorar la prevención, la detección y el análisis, así como la capacidad para responder a los problemas e incidentes de ciberseguridad; ayudar a los Estados miembros, a petición suya, en el desarrollo de CSIRT nacionales y de estrategias nacionales de ciberseguridad; ayudar a las instituciones de la Unión en la elaboración y revisión de las estrategias de ciberseguridad de la Unión; organizar formación en materia de ciberseguridad; ayudar a los Estados miembros, a través del Grupo de cooperación, en el intercambio de mejores prácticas; facilitar la creación de centros sectoriales de puesta en común y análisis de la información (ISAC).

El apoyo a la cooperación operativa y la gestión de crisis: Apoyar la cooperación entre los organismos públicos competentes y entre las partes interesadas mediante el establecimiento de una cooperación sistemática con las instituciones, órganos y organismos de la Unión que se ocupan de la ciberseguridad, la ciberdelincuencia y la protección de la intimidad y de los datos personales; encargarse de la secretaría de la red de CSIRT (artículo 12, apartado 2, de la Directiva (UE) 2016/1148) y contribuir a la cooperación operativa dentro de la red, prestando, en cooperación con el CERT-UE, apoyo a los Estados miembros, a petición suya; organizar periódicamente ejercicios de ciberseguridad; contribuir al desarrollo de una respuesta cooperativa a los incidentes y crisis de ciberseguridad transfronterizos y a gran escala; llevar a cabo, en cooperación con la red de CSIRT, investigaciones técnicas *ex post* sobre los incidentes importantes y emitir recomendaciones de seguimiento.

Las tareas relacionadas con el mercado (normalización, certificación): Desempeñar una serie de funciones que respalden específicamente el mercado interior: «observatorio del mercado» de la ciberseguridad, analizando las tendencias pertinentes en dicho mercado para adecuar mejor la oferta y la demanda; apoyar y promover el desarrollo y la aplicación de la política de la Unión sobre certificación de la ciberseguridad de productos y servicios de TIC, preparando propuestas de regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, encargándose de la secretaría del Grupo de Certificación

[44] La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

de la Ciberseguridad de la Unión y proporcionando directrices y buenas prácticas relativas a los requisitos de seguridad de los productos y servicios de TIC en cooperación con las autoridades nacionales de supervisión de la certificación y la industria. **Un mayor apoyo a los conocimientos, la información y la sensibilización**: Prestar asistencia y asesorar a la Comisión y a los Estados miembros para alcanzar un elevado nivel de conocimientos, en toda la Unión, sobre las cuestiones relacionadas con la SRI y su aplicación a las partes interesadas de la industria. Esto supone también la puesta en común, la organización y la puesta a disposición del público, a través de un portal asignado a este propósito, de información sobre seguridad de las redes y los sistemas de información [o ciberseguridad]. Otro elemento importante son las actividades de sensibilización y campañas de información destinadas al público en general sobre los riesgos en materia de ciberseguridad.

Un mayor apoyo a la investigación y la innovación: Proporcionar asesoramiento sobre las necesidades de investigación y el establecimiento de prioridades en el ámbito de la ciberseguridad.

El apoyo a la cooperación internacional: Apoyar los esfuerzos de la Unión por cooperar con terceros países y con organizaciones internacionales a fin de promover la cooperación internacional en materia de ciberseguridad.

CERTIFICACIÓN

El marco de certificación contribuirá al logro de los objetivos incrementando la transparencia general de la garantía de ciberseguridad[45] de los productos y servicios de TIC y, por ende, reforzando la confianza en el mercado único digital y en la innovación digital. Esto contribuirá también a evitar la fragmentación de los regímenes de certificación en la UE, así como de los requisitos de seguridad y criterios de evaluación conexos en los distintos Estados miembros y sectores.

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

Se espera que una ENISA reforzada, que preste apoyo a las capacidades, la prevención, la cooperación y la sensibilización a nivel de la UE, diseñada por tanto para aumentar la ciberresiliencia global de la UE, y respalde asimismo el marco europeo de certificación de productos y servicios de TIC tenga los efectos siguientes (lista no exhaustiva):

Impacto global:

- Impacto positivo global sobre el mercado interior gracias a la reducción de la fragmentación del mercado y el aumento de la confianza en las tecnologías digitales a través de una mejor cooperación, unos enfoques más armonizados con respecto a las políticas de ciberseguridad de la UE y unas mayores capacidades a nivel de la UE. Todo ello debería dar lugar a un impacto económico positivo, ya que permitirá reducir los costes de los incidentes relacionados con la ciberseguridad / ciberdelincuencia, estimándose el impacto económico en la Unión en el 0,41 % del PIB de la UE (es decir, en torno a 55 000 millones EUR).

[45] La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

Resultados específicos:

Aumento de las capacidades y la preparación de los Estados miembros y de las empresas

- Mejora de las capacidades y la preparación de los Estados miembros en materia de ciberseguridad (gracias a análisis estratégicos a largo plazo de las ciberamenazas y los ciberincidentes, orientaciones e informes, intermediación de conocimientos especializados y buenas prácticas, disponibilidad de formación y materiales de formación, refuerzo de los ejercicios CyberEurope).

- Mejora de las capacidades de los agentes privados gracias al apoyo al establecimiento de Centros de puesta en común y análisis de la información (ISAC) en varios sectores.

- Mejora de la preparación en materia de ciberseguridad de la UE y los Estados miembros gracias a la disponibilidad de planes concertados y bien ensayados en caso de incidente de ciberseguridad transfronterizo a gran escala objeto de los ejercicios CyberEurope.

Mejora de la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE

- Mejora de la cooperación tanto dentro de los sectores público y privado como entre ellos.

- Mejora de la coherencia del enfoque con respecto a la aplicación de la Directiva SRI a través de fronteras y sectores.

- Mejora de la cooperación en el ámbito de la certificación, gracias a un marco institucional que permite el desarrollo de regímenes europeos de certificación de la ciberseguridad, así como de una política común en la materia.

Aumento de las capacidades a nivel de la UE para complementar la acción de los Estados miembros

- Mejora de la «capacidad operativa de la UE» para complementar la acción de los Estados miembros y apoyarlos, a petición suya y en relación con servicios limitados y previamente definidos. Se espera que esto tenga un efecto positivo sobre el éxito de la prevención, detección y respuesta a incidentes tanto a nivel de Estado miembro como de la Unión.

Aumento de la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad

- Mejora de los conocimientos generales de ciudadanos y empresas sobre las cuestiones relacionadas con la ciberseguridad.

- Mejora de la capacidad para tomar decisiones con conocimiento de causa sobre la compra de productos y servicios de TIC gracias a la certificación de la ciberseguridad

Fortalecimiento de la confianza en el mercado único digital y en la innovación digital mediante una mayor transparencia de la garantía de ciberseguridad de los productos y servicios de TIC

- Aumento de la transparencia de la garantía de ciberseguridad[46] de los productos y servicios de TIC gracias a la simplificación de los procedimientos para la certificación de la seguridad aportada por un marco común para la UE.

- Mejora del nivel de garantía de las propiedades de seguridad de los productos y servicios de TIC.

[46] La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

- Aumento de la utilización de la certificación de la seguridad incentivada por los procedimientos simplificados, la reducción de costes y una perspectiva de oportunidades de negocio a escala de la UE que no se ve afectada por la fragmentación del mercado.

- Mejora de la competitividad dentro del mercado de la ciberseguridad de la UE debida a la reducción de los costes y la carga administrativa para las pymes y a la eliminación de las posibles barreras a la entrada en el mercado causadas por los diversos sistemas de certificación nacionales.

Otros

- No se espera ningún impacto medioambiental significativo en relación con alguno de los objetivos.

- Con respecto al presupuesto de la UE, caben esperar mejoras de la eficiencia derivadas de la mayor cooperación y coordinación de las actividades entre las instituciones, órganos y organismos de la UE.

1.4.4. Indicadores de resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

a)

Objetivo: Aumentar las capacidades y la preparación de los Estados miembros y de las empresas:

- Número de sesiones de formación organizadas por ENISA
- Cobertura geográfica (número de países y zonas) de la asistencia directa facilitada por ENISA
- Nivel de preparación alcanzado por los Estados miembros en términos de madurez de los CSIRT y supervisión de las medidas reguladoras relacionadas con la ciberseguridad
- Número de buenas prácticas a escala de la UE para las infraestructuras críticas proporcionadas por ENISA
- Número de buenas prácticas a escala de la UE para las pymes proporcionadas por ENISA
- Publicación por ENISA de análisis estratégicos anuales de las ciberamenazas y los ciberincidentes a fin de detectar tendencias emergentes
- Contribución sistemática de ENISA a la actividad de los grupos de trabajo sobre ciberseguridad de los organismos europeos de normalización.

Objetivo: Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE:

- Número de Estados miembros que han hecho uso de las recomendaciones y dictámenes de ENISA en su proceso de formulación de políticas
- Número de instituciones, órganos y organismos de la UE que han hecho uso de las recomendaciones y dictámenes de ENISA en su proceso de formulación de políticas
- Aplicación sistemática del programa de trabajo de la red de CSIRT y buen

funcionamiento de la infraestructura de TI y los canales de comunicación de la red de CSIRT

- Número de informes técnicos puestos a disposición del Grupo de cooperación y utilizados por él
- Coherencia del enfoque con respecto a la aplicación de la Directiva SRI a través de fronteras y sectores
- Número de evaluaciones del cumplimiento de la reglamentación realizadas por ENISA
- Número de ISACS existentes en los diferentes sectores, en particular para las infraestructuras críticas
- Creación y gestión ordinaria de la plataforma de información que difunde información sobre ciberseguridad procedente de las instituciones, órganos y organismos de la UE
- Contribución sistemática a la preparación de los programas de trabajo de investigación e innovación de la UE
- Acuerdo de cooperación entre ENISA, EC3 y CERT-UE vigente
- Número de regímenes de certificación incluidos y desarrollados con arreglo al marco.

Objetivo: Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de cibercrisis transfronteriza:

- Publicación por ENISA de análisis estratégicos anuales de las ciberamenazas y los ciberincidentes a fin de detectar tendencias emergentes
- Publicación de información agregada de los incidentes notificados en virtud de la Directiva SRI por ENISA
- Número de ejercicios paneuropeos coordinados por la Agencia y número de Estados miembros y organizaciones participantes
- Número de solicitudes de apoyo a la respuesta de emergencia formuladas por los Estados miembros a ENISA y realizadas por la Agencia
- Número de análisis de vulnerabilidades, artefactos e incidentes llevados a cabo por ENISA en cooperación con el CERT-UE
- Disponibilidad de informes de situación a escala de la UE sobre la base de la información comunicada a ENISA por los Estados miembros u otras entidades en caso de ciberincidente transfronterizo a gran escala.

Objetivo: Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad:

- Realización sistemática de campañas de sensibilización a escala de la UE y nacional y actualización periódica de los temas en función de las nuevas necesidades de aprendizaje
- Aumento de la cibersensibilización entre los ciudadanos de la UE
- Realización sistemática de cuestionarios de sensibilización sobre la ciberseguridad y crecimiento a lo largo del tiempo del porcentaje de respuestas correctas
- Publicación periódica de buenas prácticas de ciberseguridad y ciberhigiene dirigida a los empleados y sus organizaciones.

Objetivo: Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la transparencia global de la garantía de ciberseguridad[47] de los productos y servicios de TIC:

- Número de regímenes que se adhieren al marco de la UE
- Reducción de los costes de obtención de un certificado de seguridad de las TIC
- Número de organismos de evaluación de la conformidad especializados en certificación de las TIC en los Estados miembros
- Creación del Grupo Europea de Certificación de la Ciberseguridad y organización de sus reuniones
- Directrices para la certificación con arreglo al marco de la UE vigente
- Publicación periódica de análisis de las principales tendencias del mercado de la ciberseguridad en la UE
- Número de productos y servicios de TIC certificados de conformidad con las normas del marco europeo de certificación de la seguridad de las TIC
- Aumento del número de usuarios finales que conocen las características de seguridad de los productos y servicios de TIC

b)

1.4.5. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

Habida cuenta de los requisitos reglamentarios y de la rápida evolución del panorama de las amenazas a la ciberseguridad, es preciso revisar el mandato de ENISA para establece un nuevo conjunto de tareas y funciones, con vistas a apoyar de manera efectiva y eficaz los esfuerzos de los Estados miembros, las instituciones de la UE y otras partes interesadas para garantizar la seguridad del ciberespacio en la Unión Europea. Se delinea el alcance propuesto del mandato, que refuerza los ámbitos en los que la agencia ha mostrado un claro valor añadido y añade otros nuevos en los que se necesita apoyo a la vista de los nuevos instrumentos y prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el plan director de ciberseguridad de la UE para la cooperación en caso de cibercrisis y la certificación de seguridad de las TIC. El nuevo mandato propuesto intenta atribuir a la Agencia funciones más sólidas y centrales, en particular respaldando también de manera más activa a los Estados miembros para hacer frente a amenazas específicas (capacidad operativa) y convirtiéndose en un centro de conocimientos especializados que asista a los Estados miembros y la Comisión en el ámbito de la certificación de la ciberseguridad.

Al mismo tiempo, la propuesta establece un marco europeo de certificación de la ciberseguridad para los productos y servicios de TIC y especifica las funciones y tareas esenciales de ENISA en el ámbito de la certificación de la ciberseguridad. Dicho Marco establece disposiciones y procedimientos comunes que permiten la creación de regímenes de certificación de la ciberseguridad a escala de la UE para productos o servicios de TIC o riesgos de ciberseguridad específicos. La creación de regímenes europeos de certificación de la ciberseguridad de conformidad con el Marco permitirá que los certificados expedidos con arreglo a dichos regímenes obtengan validez y reconocimiento en todos los Estados miembros y se combata la fragmentación actual del mercado.

[47] La transparencia de la garantía de ciberseguridad significa facilitar a los usuarios información sobre las propiedades de ciberseguridad suficiente para que puedan determinar objetivamente el nivel de seguridad de determinado producto, servicio o proceso de TIC.

1.4.6. Valor añadido de la intervención de la Unión

La ciberseguridad es un problema verdaderamente global, transfronterizo por naturaleza e intersectorial cada vez en mayor medida debido a las interdependencias entre las redes y los sistemas de información. El número, complejidad y envergadura de los incidentes de ciberseguridad, así como su impacto en la economía y la sociedad, aumentan con el paso del tiempo, y se espera que sigan haciéndolo en paralelo a la evolución de la tecnología, por ejemplo, la proliferación de la internet de las cosas. Esto implica que no cabe esperar que disminuya en el futuro la necesidad de un mayor esfuerzo común de los Estados miembros, las instituciones de la UE y las partes interesadas del sector privado para hacer frente a las amenazas a la ciberseguridad.

Desde su creación en 2004, ENISA ha tratado de fomentar la cooperación entre los Estados miembros y las partes interesadas en el ámbito de los SRI, incluyendo el apoyo a la cooperación entre los sectores público y privado. Este apoyo a la cooperación ha incluido el trabajo técnico encaminado a construir una imagen del panorama de las amenazas a escala de la UE, la creación de grupos de expertos y la organización de ejercicios paneuropeos de gestión de crisis y ciberincidentes para los sectores público y privado (en particular «Cyber Europe»). La Directiva SRI encomendó a ENISA tareas adicionales, incluida la secretaría de la red de CSIRT para la cooperación operativa entre los Estados miembros.

El valor añadido de la actuación a nivel de la UE, en particular para reforzar la cooperación entre los Estados miembros, pero también entre las comunidades SRI, fue reconocido en las Conclusiones del Consejo[48] de 2016 y también se desprende claramente de la evaluación de ENISA de 2017, que muestra que el valor añadido de la Agencia reside principalmente en su capacidad para fomentar la cooperación entre estas partes interesadas. No existe ningún otro agente a nivel de la UE que facilite la cooperación de una variedad análoga de partes interesadas en la seguridad de las redes y de la información.

El valor añadido de ENISA para acercar a las comunidades de ciberseguridad y las partes interesadas es similar en el ámbito de la certificación. El aumento de la ciberdelincuencia y de las amenazas a la seguridad ha dado lugar a la aparición de iniciativas nacionales que fijan requisitos de alto nivel en materia de certificación y ciberseguridad para los componentes de TIC utilizados en las infraestructuras tradicionales. Si bien estas iniciativas son importantes, conllevan el riesgo de provocar la fragmentación del mercado único y crear obstáculos a la interoperabilidad. Un proveedor de TIC podría tener que someterse a varios procesos de certificación si desea vender en diferentes Estados miembros. Es improbable que la ineficacia o ineficiencia de los actuales regímenes de certificación se corrija en ausencia de intervención de la UE. En ausencia de medidas, es muy probable que la fragmentación del mercado aumente en el corto a medio plazo (próximos 5-10 años) con la aparición de nuevos regímenes de certificación. La falta de coordinación y de interoperabilidad entre dichos regímenes es un elemento que reduce el potencial del mercado único digital. Esto demuestra el valor añadido de la creación de un marco europeo de certificación de la ciberseguridad para productos y servicios de TIC que instaure las condiciones adecuadas para abordar eficazmente el problema relacionado con la coexistencia de múltiples procedimientos de certificación en varios Estados miembros, reduciendo los costes de la certificación y haciendo que esta resulte más

[48] Conclusiones del Consejo: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016).

atractiva desde el punto de vista comercial y de la competencia en el conjunto de la UE.

1.4.7. Principales conclusiones extraídas de experiencias similares anteriores

De conformidad con la base jurídica de ENISA, la Comisión llevó a cabo una evaluación de la Agencia, que incluía un estudio independiente y una consulta pública. La evaluación llegó a la conclusión de que los objetivos de ENISA siguen siendo pertinentes en la actualidad. En un contexto de avances tecnológicos, evolución de las amenazas y creciente necesidad de una mayor seguridad de las redes y la información (SRI) en la UE, es preciso disponer de conocimientos técnicos sobre la evolución de las cuestiones relativas a la seguridad de las redes y de la información. Deben desarrollarse en los Estados miembros capacidades que permitan comprender las amenazas y responder a ellas, y es precisa una cooperación de las partes interesadas de todos los ámbitos temáticos e instituciones.

La Agencia ha contribuido con éxito al refuerzo de la SRI en Europa merced a la oferta de creación de capacidades en 28 Estados miembros, la mejora de la cooperación entre los Estados miembros y las partes interesadas en la SRI; y la oferta de conocimientos especializados, creación de comunidades y apoyo a la política.

Aun cuando ENISA consiguió dejar su huella, al menos en cierta medida, en el amplio campo de la SRI, no ha conseguido plenamente desarrollar una imagen sólida ni obtener visibilidad suficiente para ser reconocida como «el» centro de conocimientos especializados en Europa. La explicación reside en la amplitud de su mandato, que no estuvo acompañado de unos recursos de proporción pareja. Además, ENISA es la única agencia de la UE cuyo mandato es de duración determinada, lo que limita su capacidad para desarrollar una visión a largo plazo y apoyar a sus partes interesadas de manera sostenible. Esto contrasta también con las disposiciones de la Directiva SRI, que atribuye a ENISA tareas sin señalar fecha de finalización.

En lo que respecta a la certificación de la ciberseguridad de los productos y servicios de TIC, no existe en la actualidad ningún marco europeo. No obstante, el aumento de la ciberdelincuencia y de las amenazas a la seguridad ha dado lugar a la aparición de iniciativas nacionales, que entrañan el riesgo de fragmentación del mercado único.

1.4.8. Compatibilidad y posibles sinergias con otros instrumentos adecuados

La iniciativa es sumamente coherente con las políticas existentes, en particular en el ámbito del mercado interior. En efecto, está concebida ateniéndose al enfoque global con respecto a la ciberseguridad, tal como se define en la revisión de la Estrategia para el Mercado Único Digital, a fin de complementar un conjunto completo de medidas, tales como la revisión de la Estrategia de Ciberseguridad de la UE, el plan director de cooperación en caso de cibercrisis y las iniciativas para luchar contra la ciberdelincuencia. Garantizaría la armonía con las disposiciones de la actual legislación en materia de ciberseguridad, en particular la Directiva SRI, y se apoyaría en ella para reforzar la ciberrresiliencia de la UE mediante la mejora de las capacidades, la cooperación, la gestión de riesgos y la cibersensibilización.

Las medidas sobre certificación propuestas deberían combatir la fragmentación potencial ocasionada por los regímenes nacionales de certificación existentes y nuevos, contribuyendo al mismo tiempo al desarrollo del mercado único digital. La iniciativa también sostiene y complementa la aplicación de la Directiva SRI, proporcionando a las empresas sometidas a ella una herramienta muy útil para demostrar el cumplimiento de sus requisitos en el conjunto de la Unión.

El marco europeo de certificación de la ciberseguridad de las TIC propuesto se entiende sin perjuicio del Reglamento general de protección de datos (RGPD)[49] ni, en particular, de las disposiciones pertinentes en materia de certificación[50] aplicables a la seguridad del tratamiento de los datos personales. Por último, los regímenes propuestos en el futuro marco europeo deberían basarse en la medida de lo posible en normas internacionales como forma de evitar la creación de obstáculos para el comercio y de garantizar la coherencia con las iniciativas internacionales.

[49] Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[50] Como los artículos 42 (certificación) y 43 (organismos de certificación), así como los artículos 57, 58, y 70 que se refieren respectivamente a las funciones y competencias de las autoridades independientes de supervisión y las tareas del Comité Europeo de Protección de Datos.

1.5. Duración e incidencia financiera

☐ Propuesta/iniciativa de **duración limitada**

– ☐ Propuesta/iniciativa en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA

– ☐ Incidencia financiera desde AAAA hasta AAAA

☒ Propuesta/iniciativa de **duración ilimitada**

– Ejecución: fase de puesta en marcha desde 2019 hasta 2020,

– y pleno funcionamiento a partir de la última fecha.

1.6. Modo(s) de gestión previsto(s)[51]

☒ **Gestión directa** a cargo de la Comisión (título III – Certificación)

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

☒ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

☐ organizaciones internacionales y sus agencias (especifíquense);

☐ el BEI y el Fondo Europeo de Inversiones;

☒ los organismos a que se hace referencia en los artículos 208 y 209 (título II — ENISA);

☐ organismos de Derecho público;

☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

Observaciones

El Reglamento incluye:

- el título II del Reglamento propuesto revisa el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), atribuyéndole un papel importante en la certificación, mientras que

- el título III establece un marco para la creación de regímenes europeos de certificación de la ciberseguridad de productos y servicios de TIC, en el que ENISA desempeña un papel fundamental.

[51] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

El seguimiento se iniciará inmediatamente después de la adopción del instrumento jurídico y se centrará en su aplicación. La Comisión organizará reuniones con ENISA, representantes de los Estados miembros (por ejemplo, grupo de expertos) y partes interesadas pertinentes, en particular para facilitar la aplicación de las normas relativas a la certificación, como la creación del Consejo.

La primera evaluación tendrá lugar cinco años después de la entrada en vigor del instrumento jurídico, siempre que se disponga de datos suficientes. El instrumento jurídico incluye una cláusula explícita de evaluación y revisión [artículo XXX], en virtud de la cual la Comisión llevará a cabo una evaluación independiente. Posteriormente, la Comisión informará al Parlamento Europeo y al Consejo de su evaluación, adjuntando cuando proceda una propuesta de revisión, a fin de medir el impacto del Reglamento y su valor añadido. Las ulteriores evaluaciones deben tener lugar cada cinco años. Se aplicará la metodología de evaluación contenida en el Reglamento sobre la mejora de la legislación de la Comisión. Estas evaluaciones se llevarán a cabo con la ayuda de estudios específicos, debates de expertos y amplias consultas a las partes interesadas.

El director ejecutivo de ENISA debe presentar cada dos años al Consejo de Administración una evaluación *ex post* de las actividades de ENISA. La Agencia debe, asimismo, elaborar un plan de acción para el seguimiento de las conclusiones de las evaluaciones retrospectivas e informar cada dos años a la Comisión sobre los progresos realizados. El Consejo de Administración debe responsabilizarse de vigilar el seguimiento adecuado de dichas conclusiones.

Los supuestos casos de mala administración en las actividades de la Agencia deben estar sujetos a investigaciones del Defensor del Pueblo de conformidad con lo dispuesto en el artículo 228 del Tratado.

Las fuentes de datos para el seguimiento previsto serían principalmente ENISA, el Grupo Europeo de Certificación de la Ciberseguridad, el Grupo de Cooperación, la red de CSIRT y las autoridades de los Estados miembros. Además de los datos que se derivan de los informes (incluidos los informes anuales de actividad) de ENISA, el Grupo Europeo de Certificación de la Ciberseguridad, el Grupo de Cooperación y la red de CSIRT, se utilizarán instrumentos específicos de recogida de datos cuando sea necesario (por ejemplo, encuestas a las autoridades nacionales, Eurobarómetro e informes de la campaña del mes de la ciberseguridad y los ejercicios paneuropeos).

2.2. Sistema de gestión y de control

2.2.1. Riesgo(s) definido(s)

Los riesgos definidos son limitados: existe ya una agencia de la Unión, cuyo mandato se precisará, reforzando los ámbitos en los que ha mostrado un claro valor añadido y añadiendo otros nuevos en los que es necesario un apoyo a la vista de los nuevos instrumentos y

prioridades políticas, en especial la Directiva SRI, la revisión de la Estrategia de Ciberseguridad de la UE, el inminente plan director de ciberseguridad de la UE para la cooperación en caso de cibercrisis y la certificación de seguridad de las TIC.

La propuesta, por tanto, detalla las funciones de la Agencia y propicia mejoras de la eficiencia. El incremento de competencias operativas y tareas no representa un riesgo real en la medida en que complementaría la acción de los Estados miembros y les prestaría apoyo, previa solicitud y en relación con servicios limitados y previamente determinados.

Además, el modelo de agencia propuesto, tal como se establece en el Enfoque Común, garantiza la existencia de un control suficiente para asegurarse de que ENISA trabaja por el logro de sus objetivos. Los riesgos operativos y financieros de los cambios propuestos parecen limitados.

Al mismo tiempo, es necesario garantizar los recursos financieros adecuados para que ENISA pueda cumplir las tareas encomendadas por el nuevo mandato, en particular en el ámbito de la certificación.

2.2.2. Método(s) de control previsto(s)

Las cuentas de la agencia se someterán a la aprobación del Tribunal de Cuentas y al procedimiento de aprobación de la gestión, estando previstas auditorías.

Todas sus operaciones estarán sujetas a la supervisión del Defensor del Pueblo Europeo de conformidad con lo dispuesto en el artículo 228 del Tratado.

Véanse asimismo los puntos 2.1 y 2.2.1.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

Medidas de prevención y protección de ENISA que se aplicarán:

- El personal de la Agencia inspecciona los pagos efectuados por cualquier servicio o estudio antes de que se proceda a ningún desembolso, teniendo en cuenta las obligaciones contractuales, los principios económicos y las buenas prácticas financieras y de gestión. En todos los acuerdos y contratos celebrados entre la Agencia y los beneficiarios de pagos se incluirán disposiciones antifraude (supervisión, requisitos de información, etc.).

- Para combatir el fraude, la corrupción y otras actividades ilegales, se aplicará sin restricción lo dispuesto en el Reglamento (CE) n° 883/2013 del Parlamento Europeo y del Consejo, de 25 de mayo de 1999, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).

- La Agencia suscribirá, en un plazo de seis meses a partir del día de entrada en vigor del Reglamento, el Acuerdo Interinstitucional, de 25 de mayo de 1999, entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión de las Comunidades Europeas relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF), y adoptará sin demora las disposiciones apropiadas, que serán de aplicación a todo el personal de la Agencia.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
		CD/CND[52]	de países de la AELC[53]	de países candidatos[54]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
1a Competitividad para el crecimiento y el empleo	09.0203 ENISA y certificación de seguridad de las tecnologías de la información y las comunicaciones	CD	SÍ	NO	NO	NO
5 Gastos administrativos]	09.0101 Gastos de personal en activo de la DG de Redes de comunicaciones, contenidos y tecnología 09.0102 Gastos de personal externo en activo de la DG de Redes de comunicaciones, contenidos y tecnología	CND	NO	NO	NO	NO

52 CD = créditos disociados / CND = créditos no disociados.

53 AELC: Asociación Europea de Libre Comercio.

54 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

	09.010211 Otros gastos de gestión					

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	1a	Competitividad para el crecimiento y el empleo

ENISA			**Base de referencia** **2017 (31.12.2016)**		**2019** ***(a partir del 1.7.2019)***	**2020**	**2021**	**2022**	**TOTAL**
Título 1: Gastos de personal *(incluidos también los gastos relacionados con la contratación de personal, la formación, la infraestructura y los servicios externos)*	Compromisos	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Pagos	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Título 2: Gastos de infraestructura y funcionamiento	Compromisos	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Pagos	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Título 3: Gastos de operaciones	Compromisos	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Pagos	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTAL de los créditos para ENISA	Compromisos	=1+1 a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Pagos	=2+2 a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rúbrica del marco financiero plurianual	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

		2019 *(a partir del 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAL**
DG: CNECT						
• Recursos humanos		0,216	0,846	0,846	0,846	**2,754**
• Otros gastos administrativos		0,102	0,235	0,238	0,242	**0,817**
TOTAL DG CNECT	Créditos	0,318	1,081	1,084	1,088	**3,571**

Los costes de personal se han calculado de acuerdo con la fecha prevista de contratación (suponiendo que el empleo comienza el 1.7.2019).

La perspectiva de recursos después de 2020 es indicativa y sin perjuicio de las propuestas de la Comisión para el marco financiero plurianual posterior a 2020.

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	0,318	1,081	1,084	1,088	**3,571**

En millones EUR (al tercer decimal)

		2019	**2020**	**2021**	**2022**	**TOTAL**
TOTAL de los créditos	Compromisos	16,868	21,727	23,332	24,11	**86,038**

para las RÚBRICAS 1 a 5 del marco financiero plurianual	Pagos	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Incidencia estimada en los créditos de la Agencia

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– ☒ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAL**
Aumentar las capacidades y la preparación de los Estados miembros y de las empresas	1,408	1,900	1,931	1,969	7,208
Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE	0,939	1,266	1,288	1,313	4,806
Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de cibercrisis transfronterizas	0,704	0,950	0,965	0,985	3,604
Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad	0,704	0,950	0,965	0,985	3,604
Fortalecer la confianza en el mercado único digital y en la innovación digital mediante el refuerzo de la transparencia global de la garantía de ciberseguridad de los productos y servicios de TIC	0,939	1,266	1,288	1,313	4,806
COSTE TOTAL	4.694	6,332	6,437	6,565	24,028

[55] En este cuadro figuran únicamente los gastos operativos del título 3.

3.2.3. Incidencia estimada en los recursos humanos de la Agencia

3.2.3.1. Resumen

– ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

– ☒ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	T3/4 2019	**2020**	**2021**	**2022**
Agentes temporales (Categoría AD)	4,242	5,695	6,381	6,709
Agentes temporales (Categoría AST)	1,601	1,998	2,217	2,217
Agentes contractuales	2,041	2,041	2,041	2,041
Expertos nacionales en comisión de servicios	0,306	0,447	0,656	0,796
TOTAL	**8,190**	**10,181**	**11,295**	**11,763**

Los costes de personal se han calculado de acuerdo con la fecha prevista de contratación (para el personal actual de ENISA se asumió pleno empleo a partir de 1.1.2019). Para el nuevo personal se previó empleo progresivo a partir del 1.7.2019 para alcanzar el pleno empleo en 2022. La perspectiva de recursos después de 2020 es indicativa y sin perjuicio de las propuestas de la Comisión para el marco financiero plurianual posterior a 2020.

Incidencia estimada en el personal (ETC adicionales), plantilla de personal

Categoría y grado	2017 **ENISA actual**	T3/T4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

Total AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Total AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Total AST/SC					
TOTAL GENERAL	48	12	10	7	3

Las tareas adicionales del personal AD/AST adicional para la consecución de los objetivos del instrumento, según lo descrito en la sección 1.4.2:

Tareas	AD	AST	ENCS	Total
Política y creación de capacidades	8	1		9
Cooperación operativa	8	1	7	16
Certificación (tareas relacionadas con el mercado)	9	3	2	14
Conocimientos, información y sensibilización	1	1		2
TOTAL	26	6	9	41

Descripción de las tareas que deben llevarse a cabo:

Tareas	**Recursos adicionales necesarios**
Elaboración y ejecución de las políticas de la UE y creación de capacidades	Las tareas incluirán asistir al Grupo de cooperación, apoyar la aplicación coherente de la SRI a través de las fronteras, presentar periódicamente informes sobre el estado de la aplicación del marco jurídico de la UE; asesorar y coordinar las iniciativas sectoriales de ciberseguridad en sectores como la energía, el transporte (aviación / carretera / marítimo /

	vehículos conectados), salud o finanzas, y prestar apoyo al establecimiento de Centros de puesta en común y análisis de la información (ISAC) en varios sectores.
Cooperación operativa y gestión de crisis	**Las tareas incluirían:** Encargarse de la secretaría de la red de CSIRT garantizando, entre otras cosas, el buen funcionamiento de las infraestructuras de TI y los canales de comunicación de dicha red. Garantizar una cooperación estructurada con el CERT-UE, EC3 y otros organismos de la UE pertinentes. Organizar **ejercicios Cyber Europe**[56] - tareas relativas al paso de un evento bienal a otro anual y garantizar que los ejercicios contemplan los incidentes de principio a fin. **Asistencia técnica -** Las tareas incluirían una cooperación estructurada con el CERT-UE para proporcionar asistencia técnica en caso de incidentes significativos y para apoyar el análisis de incidentes. Para ello es preciso ofrecer a los Estados miembros asistencia para gestionar incidentes y analizar vulnerabilidades, artefactos e incidentes. Facilitar la cooperación entre Estados miembros concretos en la gestión de la respuesta de emergencia mediante un análisis y agregación de los informes de situación nacionales sobre la base de la información que los Estados miembros y otras entidades pongan a disposición de la Agencia. **Plan director para una respuesta coordinada a los ciberincidentes transfronterizos a gran escala** - La Agencia contribuirá a desarrollar una respuesta cooperativa, a nivel de la Unión y de los Estados miembros, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad a través de una serie de tareas que van desde contribuir a establecer un conocimiento de la situación a nivel de la Unión hasta someter a prueba los planes de cooperación en caso de incidentes. **Investigaciones técnicas *ex post* sobre los incidentes** - Llevar a cabo o participar en

[56] Cyber Europe es el ejercicio de ciberseguridad más grande y completo de la UE hasta la fecha, con participación de más de 700 profesionales de la ciberseguridad de los 28 Estados miembros. Se celebra cada dos años. La evaluación de ENISA y la Estrategia de Ciberseguridad de la UE de 2013 señalan que muchas partes interesadas abogan por convertir Cyber Europe en un evento anual, habida cuenta de la rápida evolución de las ciberamenazas. Sin embargo, esto no es viable por el momento, teniendo en cuenta los limitados recursos de la Agencia.

	investigaciones técnicas *ex post* sobre los incidentes en cooperación con la red de CSIRT con vistas a formular recomendaciones y reforzar las capacidades en forma de informes públicos para mejorar la prevención de incidentes futuros.
Tareas relacionadas con el mercado (normalización, certificación)	Las tareas incluirían apoyar activamente el trabajo emprendido en el marco de certificación, incluida la prestación de asesoramiento técnico para preparar propuestas de regímenes europeos de certificación de la ciberseguridad. Las tareas también incluirán el apoyo a la elaboración y aplicación de las políticas de la Unión en materia de normalización, certificación y observatorio del mercado; esto exigirá facilitar la asimilación de las normas de gestión de riesgos de los productos, redes y servicios electrónicos y asesorar a los operadores de servicios esenciales y a los proveedores de servicios digitales sobre requisitos técnicos de seguridad. Las tareas incluirán también un análisis de las principales tendencias del mercado.
Conocimientos e información, sensibilización:	Con el fin de garantizar un acceso más fácil a una información mejor estructurada sobre los riesgos en materia de ciberseguridad y las posibles soluciones, la propuesta confiere a la Agencia la nueva tarea de desarrollar y mantener la «plataforma de información» de la Unión. Se incluirían las tareas de reunir, organizar y poner a disposición del público, a través de un portal asignado a este propósito, información sobre la seguridad de las redes y los sistemas de información facilitada por las instituciones, órganos y organismos de la Unión. También incluiría el apoyo a las actividades de ENISA en el ámbito de la sensibilización para que la Agencia pueda aumentar la magnitud del esfuerzo.

3.2.3.2. Necesidades estimadas de recursos humanos para la DG matriz

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– ☒ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en valores enteros (o, a lo sumo, con un decimal)

		Personal adicional			
	Referencia 2017	T3/4 2019	2020	2021	2020
• **Empleos de plantilla (funcionarios y personal temporal)**					
09 01 01 01 (Sede y Oficinas de Representación de la Comisión)	1	2	3		
• **Personal externo (en unidades de equivalente a jornada completa: EJC)**[57]					
09 01 02 01 (AC, ENCS, INT de la dotación global)	1	2			
TOTAL		**4**	**3**		

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Representar a la Comisión en el Consejo de Administración de la Agencia. Elaborar el dictamen de la Comisión sobre el documento único de programación de ENISA y supervisar su aplicación. Supervisar la preparación del presupuesto de la Agencia y controlar su ejecución. Asistir a la Agencia en el desarrollo de sus actividades en consonancia con las políticas de la Unión, en particular mediante la participación en las reuniones pertinentes. Supervisar la aplicación del marco para los regímenes europeos de certificación de la ciberseguridad de los productos y servicios de TIC. Mantener contactos con los Estados miembros y otras partes interesadas pertinentes en lo que respecta a la labor de certificación. Cooperar con ENISA en relación con las propuestas de regímenes. Preparar propuestas de regímenes europeos de ciberseguridad.

[57] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JED = joven experto en delegación.

Personal externo	Como en el caso anterior.

3.2.4. Compatibilidad con el marco financiero plurianual vigente

– ☐ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.

– ☒ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

La propuesta implicará la reprogramación del artículo 09 02 03, debido a la revisión del mandato de ENISA, que confiere a la Agencia nuevas tareas relacionadas, entre otras cosas, con la aplicación de la Directiva SRI y del marco europeo de certificación de la ciberseguridad. Importes correspondientes:

Año	Previsión	Solicitud
2019	10,739	16,550
2020	10,954	20,646
2021	N/A	22,248*
2022	N/A	23,023*

* Se trata de una estimación. La financiación de la UE después de 2020 se examinará en el contexto de un debate a nivel de la Comisión sobre todas las propuestas para el período posterior a 2020. Esto significa que, una vez que la Comisión haya formulado su propuesta relativa al próximo marco financiero plurianual, la Comisión presentará una ficha financiera legislativa modificada que tenga en cuenta las conclusiones de la evaluación de impacto[58].

– ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[59].

3.2.5. Contribución de terceros

– ☐ La propuesta/iniciativa no prevé la cofinanciación por terceros.

– ☒ La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

[58] Enlace a la página con la evaluación de impacto

[59] Véanse los artículos 11 y 17 del Reglamento (UE, Euratom) n.° 1311/2013, por el que se establece el marco financiero plurianual para el período 2014-2020.

	Año **2019**	Año **2020**	Año **2021**	Año **2022**
AELC	p.m[60].	p.m.	p.m.	p.m.

3.3. Incidencia estimada en los ingresos

– ☒ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

  – ☐ en los recursos propios

  – ☐ en ingresos diversos

[60] El importe exacto para los años siguientes se conocerá en el momento en que se fije el factor de proporcionalidad de la AELC para el año de que se trate.

COMISIÓN
EUROPEA

Bruselas, 13.9.2017
SWD(2017) 501 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. NECESIDAD DE ACTUAR

¿Cuál es el problema y por qué lo es?

Las tecnologías digitales e internet constituyen la espina dorsal de la economía y de la sociedad de la UE. Sectores económicos vitales, como el transporte, la energía, la salud o las finanzas, se han vuelto cada vez más dependientes de las redes y los sistemas de información para llevar a cabo sus actividades principales. La internet de las cosas conecta objetos y personas a través de las redes de comunicación. Esta nueva realidad crea oportunidades sin precedentes, pero también puntos vulnerables. Y ciertamente el número de ciberincidentes se dispara. Su complejidad, su frecuencia y la «superficie» de su impacto (desde el acceso a los servicios esenciales a los procesos democráticos) no van a dejar de aumentar.

En este contexto, se han detectado los siguientes problemas interrelacionados:

- fragmentación de las políticas y enfoques en materia de ciberseguridad en los distintos Estados miembros;
- dispersión de los recursos y enfoques en materia de ciberseguridad en las instituciones, órganos y organismos de la UE;
- conocimiento insuficiente de las ciberamenazas por parte de ciudadanos y empresas e información insuficiente sobre las propiedades de seguridad de los productos y servicios de TIC que adquieren, junto con la creciente aparición de múltiples regímenes de certificación nacionales y sectoriales.

Estos problemas repercuten en la ciberrresiliencia global de la UE, así como en el buen funcionamiento del mercado interior.

¿Qué se pretende conseguir?

Los objetivos políticos específicos de la presente iniciativa son los siguientes:

1. Aumentar las capacidades y la preparación de los Estados miembros y de las empresas, en particular en lo referente a las infraestructuras críticas.
2. Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE.
3. Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de cibercrisis transfronteriza.
4. Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad.
5. Aumentar en general la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC, a fin de reforzar la confianza en el mercado único digital y en la innovación digital.
6. Evitar la fragmentación, en los distintos Estados miembros y sectores, de los sistemas de certificación en la UE y los requisitos de seguridad y criterios de evaluación conexos.

¿Cuál es el valor añadido de la actuación a nivel de la UE?

Dado que la digitalización y la interconexión de la economía y la sociedad tienen un alcance global, la dimensión de los problemas va mucho más allá del territorio de un solo Estado miembro. Ello exige, por tanto, una intervención a nivel de la Unión. En el contexto actual, y teniendo en cuenta las hipótesis sobre el futuro, parece que las acciones individuales de los Estados miembros y un enfoque fragmentado en materia de ciberseguridad, vista sobre todo su importante dimensión transfronteriza, no pueden incrementar la ciberresiliencia colectiva de la Unión.

B. SOLUCIONES

¿Cuáles son las distintas opciones posibles para alcanzar los objetivos? ¿Existe o no una opción preferida?

La presente evaluación de impacto examina una serie de opciones políticas, que abarcan la revisión de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) y la certificación de seguridad de las TIC.

Revisión de ENISA

Opción 0 - **Hipótesis de referencia** - Esta opción consiste en el mantenimiento del *statu quo*. Se prorrogaría el mandato de ENISA y los objetivos y cometidos de la Agencia se mantendrían básicamente sin cambios, teniendo al mismo tiempo en cuenta las tareas encomendadas a ENISA por la legislación posterior de la UE (por ejemplo, la Directiva SRI).

Opción 1 - **Expiración del mandato de ENISA** (fin de ENISA). Esta opción pondría fin a ENISA al concluir su mandato (junio de 2020) y supondría posiblemente una redistribución de competencias/actividades a nivel de la UE o nacional.

Opción 2 - **Reforma de ENISA**. Esta opción partiría del actual mandato de ENISA, con vistas a adoptar modificaciones selectivas que tengan en cuenta la evolución del panorama de la ciberseguridad. La Agencia obtendría un mandato permanente, basado en los siguientes pilares: apoyo a la elaboración y ejecución de las políticas de la UE; creación de capacidades; conocimientos e información; tareas relacionadas con el mercado; investigación e innovación; y cooperación operativa y gestión de crisis.

Opción 3 - **Una agencia de ciberseguridad de la UE con plena capacidad operativa**. Esta opción supone reformar ENISA reuniendo tres funciones principales: 1. Una función política/consultiva; 2. Un centro de información y conocimientos, y 3. Un equipo de respuesta a emergencias informáticas (CERT). En gran medida, esta opción implicaría el mismo cambio en el alcance del mandato que la opción 2. Sin embargo, podrían incluirse tareas adicionales en el ámbito de la gestión de crisis y de respuesta a incidentes, con el fin de que la Agencia pudiera cubrir todo el ciclo de vida de la ciberseguridad y abordar la prevención, detección y respuesta a ciberincidentes.

Certificación

Opción 0 - **Hipótesis de referencia - no hacer nada**. Con arreglo a esta opción, la Comisión mantendría el *statu quo* y no emprender ninguna acción legislativa ni política.

<u>Opción 1</u> - **Medidas no legislativas (Derecho indicativo)**. Con arreglo a esta opción, la Comisión utilizaría instrumentos políticos flexibles (por ejemplo, comunicaciones interpretativas, apoyo a las iniciativas de autorregulación y las actividades de normalización a escala de la UE) a fin de mejorar la transparencia y reducir la fragmentación.

<u>Opción 2</u> - **Un acto legislativo de la UE para hacer extensivo a todos los Estados miembros el acuerdo SOG-IS**. Con arreglo a esta opción, la Comisión propondría un acto legislativo para incluir jurídicamente a todos los Estados miembros.

<u>Opción 3</u> - **Un marco general de certificación de la ciberseguridad de las TIC en la UE**. Esta opción implica el establecimiento de un marco europeo de certificación de la seguridad de las TIC (incluido un grupo de expertos compuesto por autoridades nacionales), apoyándose en la medida de lo posible en los regímenes de certificación de la seguridad de las TIC ya existentes. En esencia, el marco permitiría el establecimiento de regímenes de certificación de la UE aceptados en todos los Estados miembros.

La opción preferida es una combinación de la opción 2 para ENISA y de la opción 3 para la certificación.

¿Cuáles son las distintas partes interesadas? ¿Quién apoya cada opción?

La gran mayoría de las partes interesadas de todas las categorías (Estados miembros, industria, instituciones de la UE, comunidad investigadora) que participaron en las consultas parece a favor de la opción preferida, ya que supone reforzar ENISA y crear un marco europeo de certificación de la seguridad de las TIC.

En particular, existe consenso sobre la necesidad de disponer (como mínimo) de una agencia de la UE que funcione correctamente con un mandato permanente y cuente con los recursos y el mandato adecuados para hacer frente a los retos actuales y futuros en materia de ciberseguridad. También existe un amplio consenso entre las partes interesadas sobre la creación de un marco europeo voluntario y modulable.

En la industria, esta solución para la certificación está respaldada por las empresas que ya están sujetas a requisitos de certificación, a las que favorecería un mecanismo a escala de la UE basado en el reconocimiento mutuo de certificados. También la apoyan las pymes, que son las que más sufren cuando tienen que embarcarse en diferentes procesos de certificación en distintos Estados miembros o sufrirían si tuvieran que hacerlo. Algunos Estados miembros, en particular los que disponen de menos recursos, y algunos representantes de la industria y de las instituciones de la UE también manifestaron una opinión positiva por lo que se refiere a la opción 3 para ENISA.

C. REPERCUSIONES DE LA OPCIÓN PREFERIDA

¿Cuáles son las ventajas de la opción preferida (si existe, o bien de las principales)?

En el marco de la opción preferida, la UE dispondría de una agencia centrada en prestar apoyo a los Estados miembros, las instituciones de la UE y de las empresas en las áreas donde pudiera aportar más valor añadido. Se trataría de: apoyo a la aplicación de la Directiva SRI; elaboración y ejecución de políticas; información, conocimientos y sensibilización; investigación; cooperación operativa y gestión de crisis; mercado. En particular, ENISA

apoyaría la política de la UE en el ámbito de la certificación de la seguridad de las TIC, velando por el mantenimiento administrativo y la gestión técnica de un marco europeo de certificación de seguridad de las TIC. Dicho marco establecería de manera efectiva un conjunto de normas sobre la gobernanza de la certificación de la seguridad de las TIC en la UE, que promovería un régimen de reconocimiento mutuo de los certificados expedidos en todos los Estados miembros. La solución que combina estas opciones se considera la más eficaz para que la UE alcance los objetivos señalados de: aumentar las capacidades de ciberseguridad; preparación; cooperación; sensibilización; transparencia; y evitación de la fragmentación del mercado. Esta opción es también la más coherente con las prioridades políticas, tal como se consagran en la Estrategia de Ciberseguridad y medidas conexas (por ejemplo, la Directiva SRI), y en la Estrategia para el Mercado Único Digital. Además, esta opción permitiría alcanzar los objetivos mediante un empleo razonable de los recursos.

¿Cuáles son los costes de la opción preferida (si existe, o bien de las principales)?

Pese a la adquisición de nuevas funciones, la «ENISA reformada» seguirá siendo una organización ágil. La contribución financiera del presupuesto de la UE necesaria sería superior a la actual, pero seguiría bastante por debajo de otras agencias que también operan en áreas críticas.

La creación de un marco europeo de certificación de la seguridad de las TIC no implicaría costes adicionales iniciales para la industria (incluidas las pymes). Supondría al contrario un ahorro considerable para las empresas que ya certifican sus productos o están dispuestas a efectuar la certificación de la seguridad, con repercusiones positivas para su competitividad en el mundo. Por otro lado, implicaría a algunos compromisos presupuestarios para garantizar el mantenimiento del marco, que deberían proceder en su mayor parte del modelo de la «ENISA reformada», en lo que se refiere a las tareas técnicas y de secretaría.

¿Habrá repercusiones significativas en los presupuestos y las administraciones nacionales?

No. Los costes asociados al refuerzo de ENISA serían principalmente con cargo al presupuesto de la UE, aunque los Estados miembros aún podrían aportar contribuciones financieras voluntarias a la Agencia. En cuanto a la certificación, las principales repercusiones sobre los presupuestos y la administración nacionales derivarían de la creación de una autoridad de certificación, en su caso.

¿Habrá otras repercusiones significativas?

No

Proporcionalidad

La opción preferida incluye medidas equilibradas, todas ellas consideradas necesarias para alcanzar los objetivos previstos, sin por ello imponer una carga excesiva a los interesados. En vista de ello, se considera que la presente iniciativa se ajusta al principio de proporcionalidad.

D. SEGUIMIENTO

¿Cuándo se revisará la política?

Se propone ahora que la primera evaluación tenga lugar cinco años después de la entrada en vigor del instrumento jurídico. Posteriormente, la Comisión informará al Parlamento Europeo y al Consejo sobre su evaluación, adjuntando cuando proceda una propuesta para su revisión. Se llevarán a cabo evaluaciones posteriores cada cinco años.

Asunto: Propuesta de REGLAMENTO DEL CONSEJO por el que se modifica el Reglamento (UE) n.º 904/2010 en lo que se refiere al sujeto pasivo certificado [COM(2017) 567 final] [2017/0248 (CNS)]

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo de que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

SECRETARÍA DE LA COMISIÓN MIXTA PARA LA UNIÓN EUROPEA

COMISIÓN
EUROPEA

Bruselas, 4.10.2017
COM(2017) 567 final

2017/0248 (CNS)

Propuesta de

REGLAMENTO DEL CONSEJO

por el que se modifica el Reglamento (UE) n.º 904/2010 en lo que se refiere al sujeto pasivo certificado

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente propuesta forma parte del paquete legislativo destinado a introducir un régimen definitivo del IVA aplicable al comercio transfronterizo dentro de la Unión basado en el principio de imposición en el Estado miembro de destino de las mercancías, con el fin de crear un espacio europeo de aplicación del IVA único y sólido. En el Programa de Trabajo de la Comisión para 2017[1], se incluyó una propuesta legislativa que contemplaba la adopción de un régimen definitivo del IVA más sencillo y a prueba de fraudes para el comercio dentro de la Unión. Estas propuestas en favor de la adopción de un régimen definitivo del IVA para el comercio transfronterizo dentro de la Unión también incluyen mejoras del régimen actual del IVA, en respuesta a la solicitud de los Estados miembros[2].

Tanto en lo que atañe al régimen definitivo de IVA como por lo que se respecta a algunas de las citadas mejoras del régimen actual, los sujetos pasivos deberían poder obtener el estatuto de sujeto pasivo certificado en determinadas condiciones. El concepto de sujeto pasivo certificado debería permitir expedir una certificación que acredite que una determinada empresa tiene globalmente la consideración de sujeto pasivo fiable. Algunas de las normas de simplificación relacionadas con los acuerdos de existencias de reserva, las operaciones en cadena y la prueba del transporte de los bienes transportados o expedidos a otro Estado miembro que podrían ser vulnerables al fraude solo deberían aplicarse cuando en la operación de que se trate intervengan sujetos pasivos certificados. El concepto de sujeto pasivo certificado permitiría asimismo una aplicación gradual del régimen definitivo del IVA, en la medida en que, durante la primera fase de dicho régimen, la inversión del sujeto pasivo se aplicaría cuando el adquiriente, en el caso de entregas de bienes dentro de la Unión, sea un sujeto pasivo certificado. La justificación es que, dado que un sujeto pasivo certificado es por definición un sujeto pasivo fiable, no debería producirse ningún fraude como consecuencia de no aplicar el IVA a determinadas entregas de bienes dentro de la Unión realizadas en favor de un sujeto pasivo certificado.

En este contexto, es esencial para las empresas y las administraciones fiscales que el estatuto de sujeto pasivo certificado de una empresa pueda ser comprobado de forma inmediata y en línea. A tal efecto, es necesario que todos los Estados miembros almacenen información sobre las empresas y su estatuto de sujeto pasivo certificado en un sistema electrónico, y que las autoridades competentes de cada Estado miembro garanticen que es posible obtener la confirmación de este estatuto con respecto a cualquier empresa. Estas obligaciones de los Estados miembros se establecerán en el marco de la legislación sobre cooperación administrativa, es decir, el Reglamento (UE) n.º 904/2010 del Consejo, de 7 de octubre de 2010, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido[3] (en lo sucesivo, «el Reglamento de cooperación administrativa en materia de IVA»).

---

1 Programa de Trabajo de la Comisión para 2017: Realizar una Europa que proteja, capacite y vele por la seguridad, COM(2016) 710 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1487237841093&uri=CELEX:52016DC0710

2 Conclusiones del Consejo, de 8 de noviembre de 2016, sobre la mejora de las normas vigentes de la UE sobre el IVA aplicables a las operaciones transfronterizas (n.º 14257/16 FISC 190 ECOFIN 1023 de 9 noviembre de 2016). http://data.consilium.europa.eu/doc/document/ST-14257-2016-INIT/en/pdf

3 DO L 268 de 12.10.2010, pp. 1–18.

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La propuesta tiene por objeto dar un efecto útil al estatuto de sujeto pasivo certificado, que es un componente básico del régimen definitivo del IVA para el comercio dentro de la Unión basado en el principio de imposición en el Estado miembro de destino de las mercancías, tal como se anunció en el Plan de Acción del IVA[4]. Dicho estatuto es igualmente pertinente con relación a determinadas mejoras del actual régimen solicitadas por los Estados miembros, especialmente en lo que se refiere a las normas que regulan las operaciones en cadena, las situaciones de existencias de reserva y la prueba del transporte en las entregas intracomunitarias de bienes exentas.

- **Coherencia con otras políticas de la Unión**

La creación de un régimen del IVA simple, moderno y a prueba de fraude es una de las prioridades fiscales fijadas por la Comisión para 2017[5].

La lucha contra el fraude del IVA del operador desaparecido es también una de las prioridades de lucha contra la delincuencia de la Unión Europea, en el marco del ciclo de actuación de la UE 2014-2017 de Europol[6]. También puede hacerse referencia al acuerdo[7] relativo a la creación de la Fiscalía Europea (EPPO), llamada, en determinadas condiciones, a ocuparse del fraude del IVA.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- **Base jurídica**

La propuesta se basa en el artículo 113 del Tratado de Funcionamiento de la Unión Europea (TFUE). Dicho artículo dispone que el Consejo, por unanimidad con arreglo a un procedimiento legislativo especial, y previa consulta al Parlamento Europeo y al Comité Económico y Social, adoptará las disposiciones referentes a la armonización de la normativa de los Estados miembros en el ámbito de los impuestos indirectos.

- **Subsidiariedad (en el caso de competencia no exclusiva)**

Según el principio de subsidiariedad, establecido en el artículo 5, apartado 3, del Tratado de la Unión Europea, solo debería actuarse a escala de la UE cuando los objetivos perseguidos no puedan ser alcanzados de manera satisfactoria por los Estados miembros individualmente y, por consiguiente, debido a las dimensiones o los efectos de la acción propuesta, pueda alcanzarlos mejor la UE.

Las cuestiones relacionadas con el almacenamiento y el permiso de acceso a la información relativa al estatuto de sujeto pasivo certificado de las empresas no puede, por su naturaleza, ser decididas por los Estados miembros a título individual dado que tanto las empresas como las administraciones fiscales de todos los Estados miembros deberían, de forma normalizada, poder comprobar el estatuto de sujeto pasivo certificado de las empresas establecidas en otros Estados miembros. Esto exige un marco común, y una iniciativa en este sentido requiere una propuesta de la Comisión para modificar el Reglamento de cooperación administrativa en materia de IVA.

---

4 Plan de acción sobre el IVA — Hacia un territorio único de aplicación del IVA en la UE - Es hora de decidir [COM(2016) 148 final de 7 de abril de 2016].

5 Estudio Prospectivo Anual sobre el Crecimiento 2017, véase https://ec.europa.eu/info/publications/2017-european-semester-annual-growth-survey_en

6 Prioridades EMPACT (European multidisciplinary platform against criminal threats).

7 Véase http://www.consilium.europa.eu/en/press/press-releases/2017/06/08-eppo/

- **Proporcionalidad**

La propuesta se limita a definir un marco en relación con el estatuto de sujeto pasivo certificado, mientras que el control operativo y las medidas de aplicación siguen siendo responsabilidad de los Estados miembros. En particular, la concesión o denegación del estatuto de sujeto pasivo certificado a los contribuyentes individuales, sobre la base de las condiciones acordadas, sigue siendo competencia exclusiva de los Estados miembros.

- **Elección del instrumento**

Como el acto legislativo vigente es un reglamento, solo puede ser modificado por otro reglamento.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Consultas con las partes interesadas**

La Comisión ha creado dos grupos de trabajo para los debates técnicos en materia de IVA, a saber, el Grupo sobre el futuro del IVA (GFV, por *Group on the Future of VAT*), y el Grupo de expertos sobre el IVA (VEG, por *VAT Expert Group*). Estos grupos han debatido sobre el régimen definitivo del IVA para el comercio dentro de la Unión, incluido el concepto de sujeto pasivo certificado. Además, se organizó una consulta pública entre el 20 de diciembre de 2016 y el 20 de marzo de 2017, que contó con 121 contribuciones[8].

- **Evaluación de impacto**

Se hace referencia a la evaluación de impacto separada [SWD(2017)325 y su resumen SWD(2017)326] realizada, en particular, con relación a la presente propuesta.

La evaluación de impacto que acompaña a la presente propuesta fue examinada por el Comité de Control Reglamentario el 14 de julio de 2017 [Ares(2017)3573962-SEC(2017)423]. El Comité emitió un dictamen favorable a la propuesta con algunas recomendaciones que han sido tenidas en cuenta. El dictamen del Comité y las recomendaciones se recogen en el anexo 1 del documento de trabajo de los servicios de la Comisión correspondiente a la evaluación de impacto que se adjunta a la presente propuesta.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene ninguna incidencia en el presupuesto de la Unión.

5. OTROS ELEMENTOS

- **Explicación detallada de las disposiciones específicas de la propuesta**

El objetivo del artículo 1 de la propuesta es proporcionar la base para la integración del estatuto de sujeto pasivo certificado en el sistema VIES (sistema de intercambio de

[8] Sobre la consulta de las partes interesadas, véase el anexo 2 del documento de trabajo de los servicios de la Comisión - Evaluación de impacto que acompaña al documento «Propuesta de Directiva del Consejo por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros», y los resultados de la consulta pública abierta: https://ec.europa.eu/taxation_customs/consultations-get-involved/tax-consultations_en

información sobre el IVA). En la actualidad, el sistema VIES se utiliza, entre otras cosas, para comprobar la validez del número a efectos del IVA de un cliente en otro Estado miembro con el fin de determinar que una entrega de bienes transportados o expedidos a dicho cliente fuera del Estado miembro de entrega puede estar exenta del IVA. Desde un punto de vista práctico, la comprobación del estatuto de sujeto pasivo certificado del cliente a fin de no aplicar el IVA en el caso de una entrega de bienes al amparo del régimen definitivo es bastante similar a la comprobación de un número de identificación a efectos del IVA. Dado que el estatuto de sujeto pasivo certificado es pertinente en situaciones transfronterizas, y dado que la infraestructura informática ya ha sido implantada y utilizada por todas las administraciones fiscales, es oportuno utilizar las infraestructuras existentes y ampliar su funcionamiento a fin de incluir el estatuto de sujeto pasivo certificado de los sujetos pasivos.

Para integrar el estatuto de sujeto pasivo certificado, es necesario, en primer lugar, que los Estados miembros, que son responsables de la concesión y retirada de dicho estatuto a las empresas establecidas en su territorio, recopilen esta información y la almacenen electrónicamente. Con este propósito, el artículo 17 del Reglamento de cooperación administrativa en materia de IVA se modifica para garantizar que también se almacene información sobre el estatuto de sujeto pasivo certificado de los sujetos pasivos. Por otra parte, mediante una ulterior adaptación del artículo 31 del Reglamento de cooperación administrativa en materia de IVA, se garantiza que la confirmación del estatuto de sujeto pasivo certificado de un particular puede obtenerse por medios electrónicos.

2017/0248 (CNS)

Propuesta de

REGLAMENTO DEL CONSEJO

por el que se modifica el Reglamento (UE) n.º 904/2010 en lo que se refiere al sujeto pasivo certificado

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 113,

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Parlamento Europeo[1],

Visto el dictamen del Comité Económico y Social Europeo[2],

De conformidad con un procedimiento legislativo especial,

Considerando lo siguiente:

1. En su Plan de Acción del IVA[3], la Comisión anunció su intención de presentar una propuesta que sentara los principios para un régimen definitivo del impuesto sobre el valor añadido (IVA) aplicable al comercio transfronterizo entre empresas de los Estados miembros. El Consejo, en sus conclusiones de 8 de noviembre de 2016[4], invitó a la Comisión a introducir entretanto ciertas mejoras en las normas de la Unión en materia de IVA aplicables a las operaciones transfronterizas.

2. El concepto de sujeto pasivo certificado es uno de los componentes esenciales de este nuevo régimen definitivo del IVA para el comercio dentro de la Unión y se utilizará, además, para articular determinadas medidas de simplificación del actual régimen del IVA. El concepto de sujeto pasivo certificado debería permitir probar que un sujeto pasivo concreto puede ser considerado un sujeto pasivo fiable dentro de la Unión.

3. Determinadas normas establecidas en la Directiva 2006/112/CE[5] aplicables a las operaciones que se consideran vulnerables al fraude solo serán de aplicación en los casos en que en la operación de que se trate participen sujetos pasivos certificados. Es fundamental, por lo tanto, que el estatuto de sujeto pasivo certificado de un sujeto pasivo pueda ser verificado por medios electrónicos, para garantizar que dichas normas puedan aplicarse.

---

1 DO C [...] de [...], p. [...].

2 DO C [...] de [...], p. [...].

3 Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo relativa a un plan de acción sobre el IVA - Hacia un territorio único de aplicación del IVA en la UE - Es hora de decidir [COM(2016)148 final, de 7 de abril de 2016].

4 Conclusiones del Consejo, de 8 de noviembre de 2016, sobre la mejora de las normas vigentes de la UE sobre el IVA aplicables a las operaciones transfronterizas (n.º 14257/16 FISC 190 ECOFIN 1023, de 9 noviembre de 2016).

5 Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido (DO L 347 de 11.12.2006, p. 1).

4. En la primera fase del camino hacia un régimen definitivo del IVA propuesto en el Plan de Acción del IVA, en el caso de las entregas de bienes dentro de la Unión, el procedimiento de la inversión del sujeto pasivo debería aplicarse cuando el adquiriente de los bienes sea un sujeto pasivo certificado. Por consiguiente, es esencial que cualquier sujeto pasivo que realice una entrega de bienes en el interior de la Unión pueda saber si su cliente ha obtenido o no el estatuto de sujeto pasivo certificado. Dada la similitud, a nivel práctico, entre este sistema y la exención actual aplicable a las entregas intracomunitarias de bienes, y a fin de evitar cargas o costes innecesarios, se debería aprovechar el actual Sistema de intercambio de información sobre el IVA (VIES), en el que debería integrarse la información sobre el estatuto de sujeto pasivo certificado.

5. A fin de suministrar información sobre el estatuto de sujeto pasivo certificado de los sujetos pasivos en los Estados miembros, los Estados miembros deberían registrar y almacenar en un sistema electrónico la información actualizada relativa al estatuto de sujeto pasivo certificado de los sujetos pasivos. Seguidamente, las autoridades fiscales de los Estados miembros deberían conceder a las autoridades fiscales de los otros Estados miembros un acceso automático a esta información, y deberían, a petición de las personas contempladas en el artículo 31, apartado 1, del Reglamento (UE) n.º 904/2010 del Consejo[6], poder confirmar por medios electrónicos el estatuto de sujeto pasivo certificado de cualquier sujeto pasivo cuando dicho estatuto sea pertinente a los efectos de las operaciones a que se hace referencia en ese artículo.

6. Teniendo en cuenta que las disposiciones incluidas en el presente Reglamento se derivan de las modificaciones introducidas por la Directiva [...]/UE del Consejo[7], el presente Reglamento debería aplicarse a partir de la fecha de aplicación de dichas modificaciones.

7. Procede, por tanto, modificar el Reglamento (UE) n.º 904/2010 en consecuencia.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El Reglamento (UE) n.º 904/2010 queda modificado como sigue:

El artículo 17 se sustituye por el texto siguiente:

«*Artículo 17*

1. Todo Estado miembro almacenará en un sistema electrónico lo siguiente:

a) la información que recoja de conformidad con el título XI, capítulo 6, de la Directiva 2006/112/CE;

b) los datos relativos a la identidad, la actividad, la forma jurídica y el domicilio de las personas a las que haya asignado un número de identificación a efectos del IVA, recogidos de conformidad con el artículo 213 de la Directiva 2006/112/CE, así como la fecha en que se asignó ese número;

---

6 Reglamento (UE) n.º 904/2010 del Consejo, de 7 de octubre de 2010, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido (DO L 268 de 12.10.2010, p. 1).

7 Directiva [...]/UE del Consejo, de [...], por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros (DO L [...]).

c) los datos relativos a los números de identificación a efectos del IVA que haya asignado y que hayan dejado de ser válidos, así como las fechas en que fueron invalidados;

d) la información que recoja de conformidad con los artículos 360, 361, 364 y 365 de la Directiva 2006/112/CE, así como, a partir del 1 de enero de 2015, la información que recoja de conformidad con los artículos 369 *quater*, 369 *septies* y 369 *octies* de dicha Directiva;

e) la información relativa al estatuto de un sujeto pasivo certificado con arreglo a lo dispuesto en el artículo 13 *bis* de la Directiva 2006/112/CE, así como a la fecha en la que dicho estatuto se ha concedido, denegado y retirado.

2. Los detalles técnicos relativos a la consulta automatizada de la información contemplada en el apartado 1, letras b), c), d) y e) del presente artículo se adoptarán de conformidad con el procedimiento contemplado en el artículo 58, apartado 2.».

2) El apartado 1 del artículo 31 se sustituye por el texto siguiente:

«1. Las autoridades competentes de cada Estado miembro velarán por que a las personas que efectúan entregas intracomunitarias de bienes o prestaciones intracomunitarias de servicios y a las personas que, siendo sujetos pasivos no establecidos, prestan servicios de telecomunicaciones, de radiodifusión y de televisión, y servicios electrónicos, en concreto aquellos enumerados en el anexo II de la Directiva 2006/112/CE, se les permita obtener, a efectos de este tipo de operaciones, confirmación por vía electrónica de la validez del número de identificación a efectos del IVA de una persona determinada, así como el nombre y la dirección correspondientes. Las autoridades competentes de cada Estado miembro harán asimismo lo necesario para que pueda comprobarse por medios electrónicos si una determinada persona es un sujeto pasivo certificado con arreglo a lo dispuesto en el artículo 13 *bis* de la Directiva 2006/112/CE, cuando ese estatuto fiscal sea pertinente a los efectos del citado artículo. Esta información deberá corresponder a los datos contemplados en el artículo 17 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.*

Se aplicará a partir del 1 de enero de 2019.

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

Hecho en Bruselas, el

Por el Consejo
El Presidente

Asunto: Propuesta de DIRECTIVA DEL CONSEJO por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros [COM(2017) 569 final] [2017/0251 (CNS) {SWD(2017) 325 final} {SWD(2017) 326 final}

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo de que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

SECRETARÍA DE LA COMISIÓN MIXTA PARA LA UNIÓN EUROPEA

COMISIÓN
EUROPEA

Bruselas, 4.10.2017
COM(2017) 569 final

2017/0251 (CNS)

Propuesta de

DIRECTIVA DEL CONSEJO

por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros

{SWD(2017) 325 final}
{SWD(2017) 326 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

Los impuestos indirectos sobre el consumo se rigen a nivel internacional por el principio fundamental de tributación en el país de destino. En otras palabras, los impuestos se aplican en el país en el que se consumen los bienes y servicios.

El impuesto sobre el valor añadido (IVA) es el impuesto sobre el consumo más antiguo de Europa. En 1967, se contrajo el compromiso de establecer un régimen definitivo del IVA que operara en el marco de la Comunidad Europea como si se aplicara en un único país[1]. La necesidad de suprimir las fronteras fiscales entre los Estados miembros antes de finales de 1992 llevó a tener que reexaminar la manera en que se gravaba el comercio de mercancías en la Comunidad Europea. El objetivo era gravar las mercancías en el país de origen, para que las mismas condiciones que se aplican al comercio nacional se aplicaran también a los intercambios intracomunitarios, reflejando plenamente la idea de un verdadero mercado interior.

Dado que aún no existían las condiciones técnicas y políticas necesarias para el establecimiento de un sistema de ese tipo, se adoptó el régimen transitorio del IVA[2]. Estas disposiciones, por lo que respecta a las operaciones comerciales entre empresas, dividen el movimiento transfronterizo de mercancías en dos operaciones distintas: una entrega exenta en el Estado miembro de partida de la mercancía, y una adquisición intracomunitaria gravada en el Estado miembro de destino. Estas normas se consideraron temporales y no están exentas de inconvenientes en la medida en que permitir que las mercancías se adquieran libres de IVA aumenta el riesgo de fraude y, al mismo tiempo, la complejidad intrínseca del sistema no es favorable al comercio transfronterizo. No obstante, este régimen transitorio sigue en funcionamiento más de 20 años después de su adopción.

Tras un amplio debate público, lanzado en el marco de una consulta en torno al «Libro Verde sobre el futuro del IVA[3]» (en lo sucesivo, «el Libro Verde») el 6 de diciembre de 2011, la Comisión adoptó la «Comunicación sobre el futuro del IVA — Hacia un sistema de IVA más simple, robusto, eficaz y adaptado al mercado único[4]». La consulta confirmó que muchas de las empresas consideran que la complejidad, los costes adicionales de cumplimiento y la inseguridad jurídica del régimen del IVA a menudo les impiden emprender actividades transfronterizas y aprovechar las ventajas del mercado único. Asimismo, brindó una oportunidad para examinar si el compromiso asumido en 1967 seguía siendo pertinente.

Los debates celebrados con los Estados miembros pusieron de manifiesto que el objetivo de la imposición en el Estado miembro de origen seguía siendo políticamente inalcanzable y este

---

1 Primera Directiva 67/227/CEE del Consejo, de 11 de abril de 1967, en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de los negocios; Segunda Directiva 67/228/CEE del Consejo, de 11 de abril de 1967, en materia de armonización de las legislaciones de los Estados Miembros relativas a los impuestos sobre el volumen de negocios - Estructura y modalidades de aplicación del sistema común de Impuesto sobre el Valor Añadido.

2 Directiva 91/680/CEE del Consejo, de 16 de diciembre de 1991, que completa el sistema común del Impuesto sobre el Valor Añadido y que modifica, con vistas a la abolición de las fronteras, la Directiva 77/388/CEE (DO L 376 de 31.12.1991, p. 1).

3 COM(2010) 695, Documento de trabajo de los servicios de la Comisión, SEC(2010) 1455 de 1.12.2010.

4 COM(2011) 851 de 6.12.2011.

extremo fue confirmado por el Consejo en mayo de 2012[5]. También el Parlamento Europeo[6] y el Comité Económico y Social Europeo[7] reconocieron la situación de punto muerto y se mostraron favorables a un nuevo régimen del IVA basado en el principio de imposición en el país de destino, como una solución realista.

Tras la adopción de la citada Comunicación, la Comisión entabló un diálogo amplio y transparente con los Estados miembros y con las partes interesadas para examinar en detalle las diferentes maneras posibles de aplicar el principio de imposición en destino. La idea principal era la de que hacer negocios en toda la Unión Europea (en lo sucesivo, «la Unión» o «la UE») debía ser algo tan simple y seguro como participar en actividades puramente nacionales. Ese diálogo se desarrolló, en particular, en el marco del Grupo sobre el futuro del IVA (GFV, por *Group on the Future of VAT*)[8] y del Grupo de expertos sobre el IVA (VEG, por *VAT Expert Group*)[9].

Tras estos debates, la Comisión adoptó, el 7 de abril de 2016, el «Plan de acción sobre el IVA – Hacia un territorio único de aplicación del IVA en la UE – Es hora de decidir[10]» (en lo sucesivo, «el Plan de Acción del IVA»). La Comisión anunció, en particular, su intención de aprobar un régimen definitivo del IVA para el comercio transfronterizo dentro de la Unión basado en el principio de imposición en el Estado miembro de destino de las mercancías, con el fin de crear un espacio europeo de aplicación del IVA único y sólido. En el Programa de Trabajo de la Comisión para 2017[11] se incluyó una propuesta legislativa que contemplaba la adopción de un régimen definitivo del IVA más sencillo y a prueba de fraudes para el comercio dentro de la Unión.

En sus Conclusiones de 25 de mayo de 2016[12], el Consejo tomó nota de los argumentos expuestos por la Comisión en su Plan de Acción del IVA para avanzar hacia un régimen definitivo del IVA y de su intención de presentar, como primer paso, una propuesta legislativa en 2017 relativa al régimen definitivo del IVA para el comercio transfronterizo entre empresas. Asimismo, reiteró su opinión de que el principio de «imposición en el Estado miembro de origen de la entrega de bienes o prestación de servicios» debe ser sustituido por

---

5 Conclusiones del Consejo sobre el futuro del IVA —reunión n.º 3167 del Consejo de Asuntos Económicos y Financieros, Bruselas, 15 de mayo de 2012 (véase en particular el punto B 4) (http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/130257.pdf).

6 Resolución del Parlamento Europeo, de 13 de octubre de 2011, sobre el futuro del IVA (P7_TA(2011)0436) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-0436

7 Dictamen del Comité Económico y Social Europeo, de 14 de julio de 2011, sobre el «Libro Verde sobre el futuro del IVA — Hacia un sistema de IVA más simple, más robusto y eficaz» http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011AE1168

8 El Grupo sobre el futuro del IVA constituye un foro de debate con los delegados especializados en el IVA de las administraciones tributarias de los Estados miembros sobre las iniciativas prelegislativas de la Comisión y un marco para el intercambio de opiniones sobre la preparación de la futura legislación en materia de IVA.

9 El Grupo de expertos sobre el IVA se compone de 40 miembros: personas físicas que posean la necesaria competencia en el ámbito del IVA y organizaciones que representen, en particular, a las empresas, los expertos fiscales y el medio universitario.

10 COM(2016) 148 final.

11 Programa de Trabajo de la Comisión para 2017: realizar una Europa que proteja, capacite y vele por la seguridad, COM(2016) 710 final http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1487237841093&uri=CELEX:52016DC0710

12 Véase: http://www.consilium.europa.eu/en/press/press-releases/2016/05/25-conclusions-vat-action-plan/

el principio de «imposición en el Estado miembro de destino». El Parlamento Europeo también acogió con satisfacción la intención de la Comisión de proponer antes de 2017 un régimen definitivo del IVA que sea sencillo, equitativo, sólido, eficiente y menos vulnerable al fraude[13].

En sus conclusiones de 8 de noviembre de 2016[14], el Consejo declaró que, mientras la Comisión está trabajando en el régimen definitivo del IVA para el comercio dentro de la Unión, convendría entretanto introducir mejoras en el actual régimen del IVA. En este contexto, el Consejo ha pedido que se introduzcan modificaciones en cuatro ámbitos:

- Número de identificación a efectos del IVA: el Consejo invitaba a la Comisión a presentar una propuesta legislativa en el sentido de que el número de identificación a efectos del IVA válido del sujeto pasivo o de una persona jurídica adquiriente de bienes no sujeta al impuesto, asignado por un Estado miembro distinto del de expedición o transporte de esos bienes, debería constituir un requisito material adicional para la aplicación de la exención en lo que se refiere a una entrega de bienes dentro de la Comunidad.
- Operaciones en cadena: el Consejo invitaba a la Comisión a proponer criterios uniformes y mejoras legislativas adecuadas que dieran lugar a una mayor seguridad jurídica y a una aplicación armonizada de las normas sobre el IVA a la hora de determinar el tratamiento a efectos del IVA de las operaciones en cadena, incluidas las operaciones triangulares.
- Existencias de reserva: el Consejo invitaba a la Comisión a proponer modificaciones de las normas vigentes en materia de IVA con el fin de permitir una simplificación y un trato uniforme de los acuerdos sobre las existencias de reserva en el comercio transfronterizo. A tal efecto, el término «existencias de reserva» se refiere a la situación en que un vendedor transfiere las mercancías a un almacén a disposición de un comprador concreto en otro Estado miembro, y dicho comprador se convierte en propietario de las mercancías en el momento de retirarlas del almacén.
- Prueba de la entrega intracomunitarias: el Consejo invitaba a la Comisión a explorar las posibilidades de un marco común de criterios recomendados para los documentos justificativos requeridos para solicitar una exención aplicable a las entregas intracomunitarias.

Con el fin de responder a la petición del Consejo, se proponen modificaciones de la Directiva sobre el IVA[15] con respecto a los tres primeros ámbitos. El cuarto ámbito requiere una

---

13 Resolución del Parlamento Europeo, de 24 de noviembre de 2016, titulada «Hacia un sistema de IVA definitivo y lucha contra el fraude en el ámbito del IVA» (2016/2033(INI)) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2016-0453

14 Conclusiones del Consejo, de 8 de noviembre de 2016, sobre la mejora de las normas vigentes de la UE sobre el IVA aplicables a las operaciones transfronterizas (n.º 14257/16 FISC 190 ECOFIN 1023 de 9 de noviembre de 2016). http://data.consilium.europa.eu/doc/document/ST-14257-2016-INIT/en/pdf

15 Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido (DO L 347 de 11.12.2006, p. 1).

modificación del Reglamento de Ejecución del IVA[16] y, por lo tanto, es objeto de una propuesta separada.

La presente propuesta introduce asimismo los pilares del régimen definitivo aplicable al comercio entre empresas dentro de la Unión. Además, una propuesta prevista para 2018 incluirá disposiciones técnicas detalladas que regulen la efectiva aplicación de estos pilares. Así pues, la primera fase legislativa del régimen definitivo del IVA anunciada en el Plan de Acción del IVA[17] incluye dos pasos: el contenido en la presente propuesta, integrado por los citados pilares, y el que tendrá lugar en 2018[18].

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La introducción de un régimen definitivo aplicable a los suministros de mercancías dentro de la UE es uno de los principales elementos del Plan de Acción del IVA Esta propuesta es un paso adelante hacia la sustitución del régimen transitorio, aplicable desde el 1 de enero de 1993, por un régimen definitivo del IVA para el comercio entre empresas dentro de la Unión en virtud del cual las operaciones nacionales y transfronterizas de bienes reciban el mismo trato[19]. Además, este régimen definitivo del IVA creará un sólido territorio único europeo de aplicación del IVA que podrá servir de apoyo a un mercado único más profundo y equitativo, el cual, a su vez, contribuirá a impulsar el empleo, el crecimiento, la inversión y la competitividad.

- **Coherencia con otras políticas de la Unión**

La creación de un régimen del IVA simple, moderno y a prueba de fraude es una de las prioridades fiscales fijadas por la Comisión para 2017[20].

La lucha contra el fraude del IVA del operador desaparecido es también una de las prioridades de lucha contra la delincuencia de la Unión Europea, en el marco del ciclo de actuación de la UE 2014-017 de Europol[21].

La reducción de la carga administrativa, en particular para las pymes, es también un objetivo importante, resaltado en la estrategia de crecimiento de la UE[22].

---

16 Reglamento de Ejecución (UE) n.º 282/2011 del Consejo, de 15 de marzo de 2011, por el que se establecen disposiciones de aplicación de la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido (refundición) (DO L 77 de 23.3.2011, p. 1).

17 El Plan de Acción del IVA establece dos medidas legislativas en relación con la introducción del régimen definitivo del IVA. Para más detalles sobre el contenido de estas medidas legislativas, véanse los dos últimos párrafos del punto 4 del Plan de Acción del IVA.

18 Puede encontrarse una descripción detallada de las fases y pasos sucesivos de la introducción del régimen definitivo del IVA en la Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo — Sobre el seguimiento del Plan de Acción del IVA — Hacia un territorio único de aplicación del IVA en la UE — Es hora de actuar (COM(2017) [...].

19 Aunque actualmente no esté en la vanguardia de los trabajos sobre el régimen definitivo del IVA, puede plantearse la necesidad de evaluar en el futuro ciertos regímenes aduaneros (por ejemplo, el CP 42) con el fin de garantizar que este principio se aplica coherentemente en combinación con los regímenes de importación/exportación.

20 Estudio Prospectivo Anual sobre el Crecimiento 2017. Véase: https://ec.europa.eu/info/publications/2017-european-semester-annual-growth-survey_en

21 Prioridades de EMPACT.

22 Europa 2020: una estrategia para un crecimiento inteligente, sostenible e integrador. Véase: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

La propuesta y sus objetivos son coherentes con la política de la UE en favor de las pymes, según lo establecido por la Iniciativa SBA (por *'Small Business Act'*)[23], y en particular con el principio de ayudar a las pymes a aprovechar en mayor medida las oportunidades que ofrece el mercado único (principio VII).

Es, además, coherente con la Estrategia para el Mercado Único[24] y los objetivos del programa de adecuación y eficacia de la reglamentación (REFIT).

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La Directiva modifica la Directiva sobre el IVA en aplicación del artículo 113 del Tratado de Funcionamiento de la Unión Europea. Dicho artículo dispone que el Consejo, por unanimidad con arreglo a un procedimiento legislativo especial, y previa consulta al Parlamento Europeo y al Comité Económico y Social, adoptará las disposiciones referentes a la armonización de la normativa de los Estados miembros en el ámbito de los impuestos indirectos.

• Subsidiariedad (en el caso de competencia no exclusiva)

Según el principio de subsidiariedad, establecido en el artículo 5, apartado 3, del Tratado de la Unión Europea, solo debería actuarse a escala de la UE cuando los objetivos perseguidos no puedan ser alcanzados de manera satisfactoria por los Estados miembros y, por consiguiente, debido a las dimensiones o los efectos de la acción propuesta, pueda alcanzarlos mejor la UE.

Por su propia naturaleza, las normas en materia de IVA para el comercio transfronterizo no pueden ser decididas por cada Estado miembro, ya que, inevitablemente, afectan a más de uno de ellos. Por otra parte, el IVA es un impuesto armonizado a nivel de la Unión y, por lo tanto, cualquier iniciativa destinada a introducir el régimen definitivo del IVA para las entregas de bienes transfronterizas requiere una propuesta de la Comisión para modificar la Directiva sobre el IVA.

Téngase en cuenta que las disposiciones para armonizar y simplificar las normas dentro del actual régimen del IVA contenidas en la presente propuesta han sido solicitadas unánimemente por los Estados miembros, lo que demuestra que la acción a nivel de la UE puede resultar más eficaz, ya que las actuaciones a nivel nacional han demostrado no ser lo bastante fructíferas.

• Proporcionalidad

La propuesta, por lo que se refiere a la introducción del régimen definitivo para los intercambios comerciales entre empresas, es conforme con el principio de proporcionalidad, es decir, no va más allá de lo que es necesario para alcanzar los objetivos de los Tratados, en particular el funcionamiento adecuado del mercado único. Al igual que en la prueba de subsidiariedad, a los Estados miembros no les es posible abordar problemas tales como el fraude o la complejidad sin una propuesta de modificación de la Directiva sobre el IVA.

---

[23] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones - «Pensar primero a pequeña escala» «Small Business Act» para Europa: iniciativa a favor de las pequeñas empresas [COM(2008) 394 final].

[24] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Mejorar el mercado único: más oportunidades para los ciudadanos y las empresas [COM(2015) 550 final] .

En cuanto a la propuesta de introducir mejoras en el actual régimen, estas son muy específicas y se limitan a un escaso número de normas en materia de IVA que han resultado difíciles de aplicar de manera sistemática y uniforme, y que han generado dificultades para los sujetos pasivos.

- **Elección del instrumento**

Se propone una Directiva con vistas a modificar la Directiva sobre el IVA.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *ex post* / control de calidad de la legislación existente**

En 2011, se encargó a un consultor externo que realizara una evaluación retrospectiva de los elementos del régimen del IVA de la Unión; los resultados de esta evaluación se han utilizado como punto de partida para el examen del actual régimen del IVA[25].

- **Consultas con las partes interesadas**

El 6 de mayo de 2011, la Comisión Europea organizó una conferencia en Milán, como parte del proceso de consulta sobre el Libro Verde. La conferencia reunió, además de al público en general, a responsables políticos, expertos, empresas y otras partes interesadas procedentes no solo de toda Europa, sino de todo mundo[26]. La consulta pública sobre el Libro Verde, que contó con unas 1 700 contribuciones, proporcionó a la Comisión una visión clara de los problemas y las posibles soluciones.

Tras la publicación del Libro Verde, la Comisión creó dos grupos de trabajo encargados de debatir el asunto a nivel técnico: el GFV y el VEG. Se celebraron en total 12 reuniones del GFV y 14 reuniones del VEG, en las que se debatieron diferentes cuestiones relacionadas con el régimen definitivo del IVA para el comercio entre empresas dentro de la Unión, así como las posibles mejoras del régimen actual. Se constituyeron varios subgrupos mixtos constituidos por miembros del GFV y del VEG encargados de tratar conjuntamente algunos temas específicos. Además, en 2015, se organizó en Viena un seminario Fiscalis[27] que reunió a miembros de ambos grupos. Se creó asimismo otro subgrupo mixto en el marco del Foro de la UE sobre el IVA[28], una plataforma de debate en la que las empresas y las autoridades competentes en materia de IVA se reúnen para debatir la forma en que la aplicación de la legislación relativa al IVA puede mejorarse en términos prácticos.

Por último, entre el 20 de diciembre de 2016 y el 20 de marzo de 2017, se organizó una consulta pública sobre el régimen definitivo para el comercio dentro de la Unión, que contó

---

25 Instituto de Estudios Fiscales (jefe de proyecto), 2011, «A retrospective evaluation of elements of the EU VAT system» (Una evaluación retrospectiva de los elementos del sistema del IVA de la UE): http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/common/publications/studies/report_evaluation_vat.pdf

26 Más información: https://ec.europa.eu/taxation_customs/business/vat/action-plan-vat/communication-future-vat/green-paper_en

27 Reglamento (UE) n.º 1286/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se establece para el período 2014-2020 un programa de acción para mejorar el funcionamiento de los sistemas fiscales de la Unión Europea (Fiscalis 2020).

28 Decisión de la Comisión, de 3 de julio de 2012, por la que se crea el Foro de la UE sobre el IVA, 2012/C198/05, (DO C 198/4 de 6.7.2012).

con 121 contribuciones[29]. El objetivo era recabar la opinión de todas las partes interesadas sobre el funcionamiento del actual régimen transitorio del IVA, las posibles mejoras a corto plazo de estas disposiciones transitorias, a tenor de la petición del Consejo, y la introducción de un régimen de IVA definitivo basado en el principio de imposición en el país de destino.

- **Obtención y uso de asesoramiento especializado**

En lo que respecta a las opciones para establecer un régimen definitivo del IVA, los siguientes estudios han proporcionado un análisis pormenorizado de los problemas que se plantean y las posibles soluciones:

- Estudio sobre la aplicación del principio actual para determinar el lugar de la prestación de servicios entre empresas a las entregas de bienes entre empresas[30].
- Estudio sobre los aspectos económicos de la aplicación del IVA a las entregas dentro de la UE de bienes y servicios[31].
- Aplicación del «principio del país de destino» a los suministros de bienes entre empresas dentro de la UE[32].
- Estudio e informes sobre la brecha del IVA en los Estados miembros de la EU-28[33].

- **Evaluación de impacto**

Se hace referencia a la evaluación de impacto separada realizada en relación con la presente propuesta. La opción preferida, elegida en esa evaluación de impacto, reduciría el fraude relacionado con el IVA transfronterizo en 41 000 millones EUR, y los costes de cumplimiento para las empresas, en 1 000 millones EUR.

La evaluación de impacto que acompaña a la presente propuesta fue examinada por el Comité de Control Reglamentario el 14 de julio de 2017. El Comité emitió un dictamen favorable a la propuesta con algunas recomendaciones, en particular sobre la relación de la propuesta con otros elementos del Plan de Acción del IVA, la necesidad de un enfoque por fases y el concepto de «sujeto pasivo certificado», que han sido tenidas en cuenta. El dictamen del Consejo y las recomendaciones se recogen en el anexo 1 del documento de trabajo de los servicios de la Comisión correspondiente a la evaluación de impacto que se adjunta a la presente propuesta.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene repercusiones negativas para el presupuesto de la Unión Europea.

---

29 Resumen de los resultados de la consulta pública abierta: https://ec.europa.eu/taxation_customs/consultations-get-involved/tax-consultations_en

30 PwC, 2012. Véase: http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/common/publications/studies/place_supply_b2b.zip

31 CPB (jefe de proyecto), 2013. Véase: https://circabc.europa.eu/sd/a/60e05641-2653-4ac3-aca2-3060896aa6e3/33-ANN%20-%20Final%20report%20-%20Study%20on%20charging%20VAT%20on%20intra-EU%20supplies%20of%20goods%20and%20services%5B1%5D.pdf

32 EY, 2015. Véase: https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/ey_study_destination_principle.pdf

33 CASE, 2016. Véase: https://ec.europa.eu/taxation_customs/sites/taxation/files/2016-09_vat-gap-report_final.pdf

5. OTROS ELEMENTOS

• Explicación detallada de las disposiciones específicas de la propuesta

Sujeto pasivo certificado: Artículo 13 *bis* [nuevo]

Esta disposición introduce el concepto de «sujeto pasivo certificado».

Por regla general, los sujetos pasivos se identifican a efectos del IVA a través de un número de identificación a tal efecto. No se distingue actualmente, a nivel de la atribución de este número, entre sujetos pasivos fiables y menos fiables. Las normas en materia de IVA, por lo que respecta a la identificación, se aplican de la misma forma a ambas categorías.

El concepto de sujeto pasivo certificado permite certificar que una determinada empresa puede ser considerada globalmente como un sujeto pasivo fiable. El concepto es importante porque algunas de las normas de simplificación, que podrían ser sensibles al fraude, solo se aplicarán cuando un sujeto pasivo certificado participe en la operación en cuestión.

Además, el concepto de sujeto pasivo certificado será uno de los elementos esenciales de la primera fase del régimen definitivo del IVA para el comercio entre empresas dentro de la Unión. El actual régimen transitorio, que contempla una entrega de bienes exenta en el Estado miembro de partida y una adquisición intracomunitaria gravada en el Estado miembro de destino, por la que el adquiriente está obligado al pago del IVA, será sustituido por el régimen definitivo, que contempla una entrega de bienes gravada a efectos del IVA en el Estado miembro de destino (la denominada entrega de bienes dentro de la Unión). El concepto del sujeto pasivo certificado permitirá una puesta en práctica gradual del régimen definitivo del IVA, puesto que, en la primera fase de aplicación de este régimen, se aplicará una inversión del sujeto pasivo (es decir, la sujeción al IVA del adquiriente y no del proveedor, lo que en la práctica genera una situación similar a la que existe en la actualidad en el marco del régimen transitorio) cuando el adquiriente, en el caso de las entregas dentro de la Unión, sea un sujeto pasivo certificado[34]. La justificación es que no debe producirse ningún fraude como consecuencia de no haberse aplicado el IVA a las entregas dentro de la Unión efectuadas por un sujeto pasivo certificado, dado que el sujeto pasivo certificado es, por definición, un contribuyente fiable.

La disposición establece los criterios generales con arreglo a los cuales los Estados miembros podrán certificar a los sujetos pasivos. Tras la adopción de la presente propuesta, deberá adoptarse un Reglamento de Ejecución del Consejo, sobre la base del artículo 397 de la Directiva sobre el IVA, a fin de organizar los aspectos prácticos del estatuto de sujeto pasivo certificado y garantizar que el procedimiento para conceder o retirar dicho estatuto esté suficientemente armonizado y normalizado en toda la Unión, de modo que pueda garantizarse una aplicación uniforme. También deberá proponerse una modificación del Reglamento de cooperación administrativa[35] para permitir integrar el estatuto de sujeto pasivo certificado en el sistema VIES (sistema de intercambio de información sobre el IVA), lo que a su vez

---

34 Según lo anunciado en el Plan de Acción del IVA, en una futura segunda fase legislativa del régimen definitivo del IVA, la fiscalidad cubriría todas las entregas transfronterizas de bienes y servicios (y, por ende, el proveedor, y no el cliente, estaría obligado al pago del IVA por todos los bienes y servicios adquiridos en otros Estados miembros), de modo que todas las entregas de bienes y servicios en el mercado único, ya sean nacionales o transfronterizas, reciban el mismo trato.

35 Reglamento (UE) n.º 904/2010 del Consejo, de 7 de octubre de 2010, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido (DO L 268 de 12.10.2010, p. 1).

permitirá tanto a las administraciones tributarias como a las empresas verificar en línea el estatuto de sujeto pasivo certificado de una determinada empresa.

Dado que la certificación de sujeto pasivo certificado implica obligaciones de información y pago con respecto al IVA, no podrán optar a ella las personas que no tengan la condición de sujeto pasivo. Por la misma razón, la propuesta excluye de la posibilidad de obtener el estatuto de sujeto pasivo certificado a los agricultores en régimen de tanto alzado, a las pymes exentas, a otros sujetos pasivos exentos sin derecho a deducción y a los sujetos pasivos ocasionales. No obstante, cualquier pyme que no aplique el sistema de exención podrá solicitar el estatuto de sujeto pasivo certificado en las mismas condiciones que cualquier otro sujeto pasivo. Por lo tanto, la propuesta es coherente con la política de la UE en el ámbito de las pymes, según lo establecido en la iniciativa SBA[36].

Existe una similitud entre los criterios que deben utilizarse para la concesión del estatuto de sujeto pasivo certificado y los aplicados en relación con el estatuto de Operador Económico Autorizado (OEA), tal y como aparece definido en el Código Aduanero de la Unión (artículo 39). También pueden hallarse criterios similares, basados en el estatuto de OEA, en la reciente propuesta sobre el IVA aplicable al comercio electrónico[37].

Existencias de reserva: artículo 17 *bis* (nuevo), artículo 243, apartado 3, y artículo 262 (modificado)

El de las existencias de reserva es un régimen en virtud del cual un proveedor transfiere bienes a un adquiriente conocido sin transferir inmediatamente la propiedad de los bienes. El adquiriente tiene derecho a retirar los bienes de una reserva del proveedor de forma discrecional, en cuyo caso tiene lugar una entrega de bienes. En las relaciones internas, el uso de este modelo no genera problemas específicos, pero se plantean dificultades cuando el proveedor y el adquiriente están establecidos en diferentes Estados miembros.

En virtud de las normas actuales sobre el IVA, cuando una empresa transfiere bienes propios a otro Estado miembro con el fin de constituir una reserva para un cliente, se considera que ha realizado una entrega de bienes exenta de IVA en el Estado miembro de partida. La llegada de las mercancías da lugar a una adquisición intracomunitaria realizada por la empresa que ha transferido las mercancías que está sujeta al IVA en ese otro Estado miembro. La empresa que ha transferido los bienes está obligada, por regla general, a estar identificada a efectos del IVA en el Estado miembro de llegada, con el fin de poder declarar la adquisición intracomunitaria en su declaración del IVA. En el momento en que las mercancías son retiradas de la reserva y entregadas al adquiriente, se produce una segunda entrega, cuyo lugar de entrega es el Estado miembro en el que la reserva está situada.

A fin de solventar las dificultades que este hecho puede generar en la práctica, algunos Estados miembros aplican medidas de simplificación a estas operaciones, pero otros no lo hacen. Estas diferencias van en contra de la aplicación uniforme de las normas sobre el IVA en el mercado único.

---

[36] Véase la nota 23.

[37] Propuesta de Directiva del Consejo por la que se modifican la Directiva 2006/112/CE y la Directiva 2009/132/CE en lo referente a determinadas obligaciones respecto del impuesto sobre el valor añadido para las prestaciones de servicios y las ventas a distancia de bienes [COM(2016) 757 final de 1.12.2016]; véase el artículo 369 *quaterdecies*, apartado 1, letra c), de la Directiva 2006/112/CE).

La solución propuesta consiste en considerar que los acuerdos relativos a las reservas de existencias dan lugar a una única entrega en el Estado miembro de partida y a una adquisición intracomunitaria en el Estado miembro en que está situada la reserva, siempre que en la operación participen dos sujetos pasivos certificados. De este modo, se evitará que el proveedor tenga la obligación de estar identificado en cada Estado miembro en el que haya introducido las mercancías en el marco del régimen de la reserva de existencias. Sin embargo, a fin de garantizar un seguimiento adecuado de las mercancías por las administraciones tributarias, tanto el proveedor como el adquiriente deberán llevar un registro de las mercancías incluidas en existencias de reserva a las que se aplican estas normas. Además, el estado recapitulativo del proveedor deberá mencionar la identidad de los adquirientes a los que los bienes serán expedidos en una fase posterior al amparo de acuerdos relativos a existencias de reserva.

Número de identificación a efectos del IVA, y exención de determinadas operaciones intracomunitarias: artículo 138, apartado 1 (modificado)

La exención del IVA para las entregas intracomunitarias de bienes contemplada en el artículo 138, apartado 1, de la Directiva sobre el IVA constituye el eje del actual régimen transitorio. Al mismo tiempo, esta exención también está en la raíz del denominado «fraude carrusel». El régimen definitivo del IVA para el comercio dentro de la Unión pretende solucionar este problema, pero, en el ínterin, los Estados miembros han pedido que se adopten soluciones provisionales. Piden, en particular, que la Directiva sobre el IVA exija un número de identificación a efectos del IVA al adquiriente en un Estado miembro distinto de aquel en el que se inicie el transporte de los bienes como un requisito material para que el proveedor pueda ser autorizado a aplicar la exención. Esta modificación transciende la situación actual, con arreglo a la cual, según la interpretación del Tribunal de Justicia de la Unión Europea[38], el número de identificación a efectos del IVA del adquiriente es simplemente una condición formal para el derecho a la exención de una entrega intracomunitaria. Esta circunstancia da actualmente lugar a situaciones en que, cuando no se ha cumplido la condición, los Estados miembros solo pueden imponer multas o sanciones administrativas, pero no denegar la exención en sí.

El régimen transitorio actual se basa, además, en la obligación para el proveedor de presentar un estado recapitulativo (la denominada «lista VIES», que incluye el número de identificación a efectos del IVA del adquiriente). Esta es también una condición para la exención no sustantiva, sino formal. A través del sistema VIES, esta información está al alcance de las autoridades fiscales del Estado miembro del adquiriente, que de este modo son informadas de la llegada a su territorio de bienes que son normalmente objeto de una adquisición intracomunitaria gravada. El adquiriente debe declarar esta adquisición intracomunitaria en su declaración IVA, y las autoridades fiscales tienen la posibilidad de cotejar esta declaración con los datos del sistema VIES. La lista VIES ha sido, pues, un elemento esencial del régimen del IVA desde la supresión de las fronteras fiscales y la consiguiente desaparición de la documentación aduanera.

A falta de una información correcta procedente del sistema VIES, las autoridades fiscales de los Estados miembros carecen de la información necesaria sobre la llegada de bienes no gravados a su territorio y dependen exclusivamente de la declaración de los sujetos pasivos.

[38] Sentencias de 6 de septiembre de 2012, Mecsek-Gabona, C-273/11, ECLI:EU:C:2012:547; de 27 de septiembre de 2012, VSTR, C-587/10, ECLI:EU:C:2012:592; de 20 de octubre de 2016, Plöckl, C-24/15, ECLI:EU:C:2016:791, y de 9 de febrero de 2017, Euro-Tyre, C-21/16, ECLI:EU:C:2017:106.

No obstante, la no inclusión de una entrega en la lista puede dar lugar a la imposición de sanciones, pero no a la denegación de la exención en sí.

Por consiguiente, el nuevo artículo 138, apartado 1, propuesto contempla cambios en estos dos aspectos. En primer lugar, mientras que actualmente se hace referencia a si el adquiriente es un sujeto pasivo o una persona jurídica no sujeta al impuesto que actúa como tal, se establece ahora, como un requisito material al que se supedita la aplicación de la exención, que el adquiriente deberá estar identificado a efectos del IVA en un Estado miembro distinto de aquel en el que se inicie la expedición o transporte de los bienes. Como ya ocurre actualmente, el proveedor deberá verificar el estatuto de su cliente a través del sistema VIES antes de aplicar la exención. Desde este punto de vista, no existe ninguna diferencia práctica para el proveedor, pero las consecuencias pueden ser diferentes, dado que la no identificación de su cliente puede, sobre esa base, dar lugar a la denegación de la exención. En segundo lugar, también la correcta inclusión en la lista VIES se convierte en un requisito material que puede conducir, de no cumplirse, al rechazo por parte de la administración tributaria de una exención ya aplicada.

Operaciones en cadena: artículo 138 *bis* (nuevo)

Las operaciones en cadena, que se consideran en el ámbito de la presente propuesta, deben entenderse como entregas sucesivas de una misma mercancía cuando los bienes entregados son objeto de un único transporte intracomunitario entre dos Estados miembros. En esta situación, según la jurisprudencia del Tribunal de Justicia[39], el transporte debe atribuirse a una entrega dentro de la cadena de suministro, a fin de determinar a cuál de las operaciones debe aplicarse la exención de entregas intracomunitarias, de conformidad con lo dispuesto en el artículo 138 de la Directiva sobre el IVA. Esta disposición establece, como requisito para la exención, que los bienes deben ser «expedidos o transportados por el vendedor, por el adquiriente o por cuenta de ellos» de un Estado miembro a otro. En este contexto, los Estados miembros han pedido que se introduzcan mejoras legislativas a fin de aumentar la seguridad jurídica de los operadores a la hora de determinar la entrega a la que, dentro de la cadena de operaciones, debe imputarse el transporte intracomunitario (que será la entrega de la cadena a se aplicará la exención prevista en el artículo 138, siempre que se cumplan todas las demás condiciones para la exención).

En caso de que el transporte haya sido realizado por o en nombre de uno de los proveedores intermediarios de la cadena, se proponen normas en virtud de las cuales dicho transporte se imputará: i) a la entrega efectuada a ese proveedor intermediario si este está, a efectos del IVA, identificado en un Estado miembro distinto del Estado miembro de entrega y ha comunicado el nombre del Estado miembro de llegada de las mercancías a su proveedor; ii) a la entrega efectuada por el proveedor intermediario al siguiente operador de la cadena, cuando no se cumpla alguna de las dos condiciones mencionadas en el punto i). Estas normas, junto con la seguridad jurídica que conllevan, únicamente se aplicarán cuando tanto el proveedor intermediario como el sujeto pasivo que efectúa la entrega de bienes sean sujetos pasivos certificados. No se necesitará ninguna norma de este tipo cuando el transporte se realice en nombre del primer proveedor de la cadena (en cuyo caso, el transporte solo puede imputarse a la primera entrega) o en nombre del último sujeto pasivo de la cadena (en cuyo caso, el transporte solo puede imputarse a la entrega efectuada por el sujeto pasivo en cuestión).

[39] Sentencia de 6 de abril de 2006, Emag Handel, C-245/04, ECLI:EU:C:2006:232.

No se excluye la posibilidad de que, en caso de participación de un sujeto pasivo que no haya sido objeto de certificación, el transporte se impute a la misma entrega. No obstante, en este caso las normas establecidas en el artículo 138 *bis* no serán de aplicación, y, como ya ocurre en las actuales condiciones, seguirá correspondiendo al sujeto pasivo interesado demostrar que el transporte y la exención están vinculadas a esa entrega concreta.

Régimen definitivo para el comercio dentro de la Unión: artículos 402 (modificado), 403 y 404 (suprimido)

Ya se han establecido los pilares del régimen definitivo para el comercio dentro de la Unión, y se han definido los principios con arreglo a los cuales se aplicará el nuevo régimen. Por lo que se refiere a la elección de este régimen particular, se hace referencia a la evaluación de impacto que acompaña a la presente propuesta.

Como ya se explica en el punto 1, una próxima propuesta de 2018 incluirá disposiciones técnicas detalladas que regulen la efectiva aplicación de estos pilares. La futura propuesta en cuestión revisará en profundidad la Directiva sobre el IVA y sustituirá o eliminará los artículos que contienen las actuales disposiciones transitorias. Para garantizar el buen funcionamiento del régimen, se precisarán otros cambios con relación a las normas de cooperación administrativa, así como importantes avances informáticos.

En la propuesta de artículo 402 de la Directiva, se establece actualmente que el régimen definitivo del IVA para el comercio dentro de la UE se basará en el principio de la imposición en el Estado miembro de destino de la entrega o prestación de los bienes y servicios. En este contexto, se introducirá en las citadas disposiciones técnicas detalladas un nuevo concepto con relación a los bienes, a saber, la denominada «entrega dentro de la Unión». Este nuevo hecho imponible único está destinado a sustituir el actual régimen de una entrega exenta en el Estado miembro de partida y una «adquisición intracomunitaria» gravada en el Estado miembro de destino como segundo e independiente hecho imponible. En el marco de este nuevo concepto, el «lugar de entrega» estará situado en el Estado miembro de destino de los bienes.

Además, el proveedor será el responsable del pago del IVA por esta entrega «dentro de la Unión» a menos que el adquiriente sea un sujeto pasivo certificado, en cuyo caso el sujeto pasivo certificado asumirá en su declaración del IVA la liquidación de este impuesto. En los casos en que el deudor del IVA no esté establecido en el Estado miembro en que se adeuda el impuesto, este tendrá posibilidad de cumplir con sus obligaciones de declaración y pago a través del denominado «sistema de ventanilla única». Este sistema también podrá utilizarse para la deducción del IVA soportado.

Aunque en esta fase esto aún no ha quedado explícitamente establecido, el sistema podría o debería basarse en mayor medida en la supresión de la declaración recapitulativa (la denominada «lista VIES»), la aplicación de las normas generales de facturación del Estado miembro del proveedor y la armonización de determinadas normas relativas a la facturación (como el momento de la expedición de las facturas), el devengo y la exigibilidad del IVA en el marco de las entregas de bienes «dentro de la UE».

2017/0251 (CNS)

Propuesta de

DIRECTIVA DEL CONSEJO

por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 113,

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Parlamento Europeo[1],

Visto el dictamen del Comité Económico y Social Europeo[2],

De conformidad con un procedimiento legislativo especial,

Considerando lo siguiente:

(1) En 1967, cuando el Consejo adoptó el sistema común del impuesto sobre el valor añadido (IVA) por medio de las Directivas 67/227/CEE[3] y 67/228/CEE[4] del Consejo, se contrajo el compromiso de establecer un régimen definitivo del IVA que operara en el marco de la Comunidad Europea como lo haría en un único Estado miembro. Dado que aún no se habían alcanzado las condiciones técnicas y políticas necesarias para el establecimiento de un régimen de ese tipo, cuando las fronteras fiscales entre los Estados miembros se suprimieron a finales de 1992 se adoptó el régimen transitorio del IVA. La Directiva 2006/112/CE[5] del Consejo, actualmente en vigor, prevé que estas disposiciones transitorias deben ser sustituidas por disposiciones definitivas.

(2) En su Plan de acción sobre el IVA[6], la Comisión anunció su intención de presentar una propuesta destinada a establecer los principios de un régimen definitivo del IVA para el comercio transfronterizo de empresa a empresa entre los Estados miembros, que se

1 DO C […] de […], p. […].

2 DO C […] de […], p. […].

3 Primera Directiva 67/227/CEE del Consejo, de 11 de abril de 1967, en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de los negocios (DO 71 de 14.4.1967, p. 1 301).

4 Segunda Directiva 67/228/CEE del Consejo, de 11 de abril de 1967, en materia de armonización de las legislaciones de los Estados Miembros relativas a los impuestos sobre el volumen de negocios - Estructura y modalidades de aplicación del sistema común de Impuesto sobre el Valor Añadido (DO 71 de 14.4.1967, p. 1 303).

5 Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido (DO L 347 de 11.12.2006, p. 1).

6 Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo relativa a un plan de acción sobre el IVA – Hacia un territorio único de aplicación del IVA en la UE – Es hora de decidir [COM(2016)148 final, de 7 de abril de 2016].

basaría en la imposición de las entregas transfronterizas de bienes en el Estado miembro de destino.

(3) Para ello, sería necesario sustituir el actual régimen, consistente en una entrega exenta en el Estado miembro de partida de los bienes y una adquisición intracomunitaria de bienes gravada en el Estado miembro de destino, por un régimen de una sola entrega gravada en el Estado miembro de destino con arreglo a sus tipos de IVA. Por regla general, el IVA será facturado por el proveedor, que podrá verificar en línea, a través de un portal web, el tipo de IVA aplicable en cualquier Estado miembro. No obstante, en caso de que el adquiriente sea un sujeto pasivo certificado (es decir, un contribuyente fiable reconocido como tal por los Estados miembros), se aplicará el mecanismo de inversión del sujeto pasivo y el sujeto pasivo certificado pasaría a ser el deudor del IVA por la entrega dentro de la Unión. El régimen definitivo del IVA se basará también en el concepto de un sistema de registro único (ventanilla única) para las empresas, en el que se podrá realizar la liquidación y la deducción del IVA adeudado.

(4) Estos principios deberían incluirse en la Directiva y sustituir el actual concepto según el cual el régimen definitivo se basará en la imposición en el Estado miembro de origen.

(5) El Consejo, en sus conclusiones de 8 de noviembre de 2016[7], invitó a la Comisión a introducir ciertas mejoras en las normas de la Unión en materia de IVA aplicables a las operaciones transfronterizas, con respecto al papel del número de identificación a efectos del IVA en el contexto de la exención de las entregas intracomunitarias, las disposiciones que regulan las existencias de reserva, las operaciones en cadena y la prueba del transporte a efectos de la exención de las operaciones intracomunitarias.

(6) Habida cuenta de esta petición, así como del hecho de que se tardará varios años en aplicar el régimen definitivo del IVA para el comercio dentro de la Unión, estas medidas específicas, destinadas a armonizar y simplificar determinadas disposiciones aplicables a las empresas, resultan adecuadas.

(7) La creación del estatuto de sujeto pasivo certificado es necesaria para la aplicación eficiente de las mejoras relativas a las normas de la Unión en materia de IVA aplicables a las operaciones transfronterizas, así como para la transición gradual hacia el régimen definitivo para el comercio dentro de la Unión.

(8) En el régimen actual, no se hace ninguna distinción entre sujetos pasivos fiables y menos fiables en relación con las normas del IVA aplicables. La concesión del estatuto de sujeto pasivo certificado sobre la base de determinados criterios objetivos debería permitir la identificación de los sujetos pasivos fiables. Este estatuto les permitiría beneficiarse de la aplicación de determinadas normas sensibles al fraude no aplicables a otros sujetos pasivos.

(9) El acceso al estatuto de sujeto pasivo certificado debería basarse en criterios armonizados a escala de la Unión y, por lo tanto, la certificación por parte de un Estado miembro debería ser válida en toda la Unión.

(10) Determinados sujetos pasivos cubiertos por regímenes particulares que los excluyen de las normas generales del IVA, o que solo ocasionalmente realizan actividades

[7] Conclusiones del Consejo, de 8 de noviembre de 2016, sobre la mejora de las normas vigentes de la UE sobre el IVA aplicables a las operaciones transfronterizas (n.º 14257/16 FISC 190 ECOFIN 1023, de 9 noviembre de 2016).

económicas, no deben poder obtener el estatuto de sujeto pasivo certificado por lo que respecta a tales regímenes particulares o actividades ocasionales. De otro modo, podría verse comprometida la correcta aplicación de las modificaciones propuestas.

(11) Las existencias de reserva hacen referencia a una situación en la que, en el momento del transporte de los bienes a otro Estado miembro, el proveedor ya conoce la identidad de la persona que adquiere los bienes, al que se entregarán en una fase posterior y tras su llegada al Estado miembro de destino. Actualmente, esta situación da lugar a una operación equiparada a una entrega (en el Estado miembro de partida de los bienes) y a una operación equiparada a una adquisición intracomunitaria en el Estado miembro de llegada de los bienes), seguidas de una entrega «nacional» en el Estado miembro de llegada, y obliga al proveedor a estar identificado a efectos del IVA en dicho Estado miembro. Para evitar esto, debe considerarse que tales operaciones, cuando tienen lugar entre dos sujetos pasivos certificados y en determinadas condiciones, dan lugar a una entrega exenta en el Estado miembro de partida y a una adquisición intracomunitaria en el Estado miembro de llegada.

(12) Por lo que se refiere al número de identificación a efectos del IVA en relación con la exención de las entregas de bienes en el comercio intracomunitario, se propone que la inclusión del número de identificación a efectos del IVA del adquiriente en el Sistema de intercambio de información sobre el IVA (VIES), asignado por un Estado miembro distinto de aquel en el que se inicie el transporte de los bienes, así como la referencia a ese número en el estado recapitulativo presentado por el proveedor deben ser, junto con la condición de que los bienes se transporten fuera del Estado miembro de entrega, requisitos no formales, sino materiales, para la aplicación de la exención. La indicación en la lista VIES es esencial para informar al Estado miembro de llegada de la presencia de los bienes en su territorio y es, por lo tanto, un elemento clave en la lucha contra el fraude en la Unión.

(13) Las operaciones en cadena se refieren a sucesivas entregas de bienes que son objeto de un único transporte intracomunitario. La circulación intracomunitaria de los bienes solo debería imputarse a una de las entregas, y solo esa entrega debería beneficiarse de la exención del IVA prevista para las entregas intracomunitarias. Las demás entregas de la cadena deberían ser objeto de gravamen y podrían requerir la identificación a efectos del IVA del proveedor en el Estado miembro de entrega. A fin de evitar planteamientos divergentes entre los Estados miembros, lo que puede dar lugar a una doble imposición o a la ausencia de imposición, y a fin de reforzar la seguridad jurídica de los operadores, conviene establecer una norma común que, siempre que se cumplan determinadas condiciones, establezca que el transporte de la mercancía debe imputarse a una entrega de la cadena de operaciones.

(14) Dado que los objetivos de la presente Directiva (la mejora del funcionamiento del régimen del IVA en el contexto del comercio transfronterizo entre empresas y la definición de los principios del régimen del IVA definitivo) no pueden alcanzarse de manera suficiente por los Estados miembros y, por consiguiente, pueden lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(15) De conformidad con la Declaración política conjunta de los Estados miembros y de la Comisión sobre los documentos explicativos[8], de 28 de septiembre de 2011, los Estados miembros se han comprometido a acompañar, en casos justificados, la notificación de sus medidas de transposición con uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos nacionales de transposición. Por lo que respecta a la presente Directiva, el legislador considera que la transmisión de tales documentos está justificada.

(16) Procede, por lo tanto, modificar la Directiva 2006/112/CE en consecuencia.

HA ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

La Directiva 2006/112/CE se modifica como sigue:

1) Se inserta el artículo 13 *bis* siguiente:

«*Artículo 13* bis

1. Cualquier sujeto pasivo que tenga su sede de actividad económica o un establecimiento permanente en la Comunidad o, en ausencia de sede de actividad económica y de establecimiento permanente, tenga su domicilio permanente o residencia habitual en la Comunidad y que, en el marco de su actividad económica, realice, o tenga la intención de realizar, alguna de las operaciones contempladas en los artículos 17 *bis*, 20 y 21, u operaciones en las condiciones especificadas en el artículo 138, podrá solicitar a la Administración tributaria el estatuto de sujeto pasivo certificado.

La Administración tributaria concederá este estatuto a un solicitante cuando se cumplan los criterios establecidos en el apartado 2, a menos que el solicitante esté excluido de esta certificación en virtud de lo dispuesto en el apartado 3.

En caso de que el solicitante sea un sujeto pasivo a quien se haya concedido el estatuto de operador económico autorizado a efectos aduaneros, se considerará que se cumplen los criterios enunciados en el apartado 2.

2. Para la concesión del estatuto de sujeto pasivo certificado, deberán cumplirse todos los criterios siguientes:

a) inexistencia de infracción grave o reiterada de la legislación aduanera y de la normativa fiscal, así como de condena por un delito grave en relación con la actividad económica del solicitante;

b) demostración, por el solicitante, de un alto nivel de control de sus operaciones y del flujo de los bienes, bien mediante un sistema de gestión de los registros comerciales y, en su caso, de los registros de transporte, que permita la correcta realización de los controles fiscales, bien mediante una pista de auditoría interna fiable o certificada;

c) prueba de la solvencia financiera del solicitante, la cual se considerará acreditada bien cuando el solicitante tenga una capacidad financiera adecuada

[8] DO C 369 de 17.12.2011, p. 14.

que le permita cumplir sus compromisos, teniendo debidamente en cuenta las características del tipo de actividad empresarial de que se trate, bien mediante la presentación de garantías aportadas por empresas de seguros u otras entidades financieras, o por otras terceras partes económicamente fiables.

3. Los siguientes sujetos pasivos no podrán obtener el estatuto de sujeto pasivo certificado:

a) los sujetos pasivos que se beneficien del régimen común de tanto alzado de los productores agrícolas;

b) los sujetos pasivos que se beneficien de la franquicia para las pequeñas empresas prevista en los artículos 282 a 292;

c) los sujetos pasivos que realicen entregas de bienes o prestaciones de servicios respecto de las cuales el IVA no sea deducible;

d) los sujetos pasivos que efectúen una entrega ocasional de un medio de transporte nuevo, en el sentido del artículo 9, apartado 2, o que lleven a cabo una actividad ocasional en el sentido del artículo 12.

No obstante, los sujetos pasivos mencionados en las letras a) a d) podrán obtener el estatuto de sujeto pasivo certificado para las otras actividades económicas que realicen.

4. Todo sujeto pasivo que solicite el estatuto de sujeto pasivo certificado deberá facilitar toda la información exigida por las autoridades tributarias para permitirles tomar una decisión.

A efectos de la concesión de este estatuto fiscal, se entenderá por 'autoridades tributarias':

a) las del Estado miembro en que el solicitante haya establecido la sede de su actividad económica;

b) las del Estado miembro donde se encuentre el establecimiento permanente del solicitante en el que se conserve o esté disponible su contabilidad principal dentro de la Comunidad a efectos fiscales, cuando el solicitante haya establecido la sede de su actividad económica fuera de la Comunidad, pero tenga uno o varios establecimientos fijos situados dentro de la Comunidad;

c) las del Estado miembro en el que el solicitante tenga su domicilio permanente o su residencia habitual, cuando no disponga ni de un centro de actividad, ni de un establecimiento permanente.

5. En caso de que la solicitud sea denegada, las autoridades tributarias comunicarán al solicitante los motivos de la denegación, junto con la propia decisión. Los Estados miembros velarán por que el solicitante disponga de un derecho de recurso contra toda decisión por la que se le deniegue una solicitud.

6. El sujeto pasivo al que se haya concedido el estatuto de sujeto pasivo certificado informará sin demora a las autoridades tributarias de cualquier circunstancia posterior a la adopción de la decisión que pueda afectar o influir en el mantenimiento de dicho estatuto. Las autoridades tributarias retirarán el estatuto fiscal cuando dejen de cumplirse los criterios establecidos en el apartado 2.

7. El estatuto de sujeto pasivo certificado concedido en un Estado miembro será reconocido por las autoridades tributarias de todos los Estados miembros.».

2) Se inserta el artículo 17 *bis* siguiente:

«Artículo 17 bis

1. La transferencia por un sujeto pasivo de un bien de su empresa con destino a otro Estado miembro en el marco de acuerdos sobre existencias de reserva no se asimilará a una entrega de bienes a título oneroso.

2. A efectos del presente artículo, se considerará que existen acuerdos sobre existencias de reserva cuando se cumplan las siguientes condiciones:

a) los bienes son expedidos o transportados a otro Estado miembro por un sujeto pasivo certificado, o por un tercero por cuenta de dicho sujeto pasivo certificado, con el fin de que esos bienes sean entregados allí, en una fase posterior y después de su llegada, a otro sujeto pasivo certificado;

b) el sujeto pasivo certificado que expide o transporta los bienes no está establecido en el Estado miembro al que se expiden o transportan los bienes;

c) el sujeto pasivo certificado destinatario de la entrega de bienes está identificado a efectos del IVA en el Estado miembro al que se transportan o expiden los bienes, y tanto su identidad como el número de identificación a efectos del IVA que le ha sido asignado por ese Estado miembro son datos conocidos por el sujeto pasivo certificado al que se refiere la letra b) en el momento del inicio de la expedición o el transporte;

d) el sujeto pasivo certificado que expide o transporta los bienes ha inscrito la expedición o el transporte en el registro contemplado en el artículo 243, apartado 3, y ha incluido en el estado recapitulativo, de conformidad con lo dispuesto en el artículo 262, tanto la identidad del sujeto pasivo certificado que adquiere los bienes como el número de identificación asignado a este último por el Estado miembro al que se expiden o transportan los bienes.

3. Cuando se cumplan las condiciones establecidas en el apartado 2, en el momento en que el derecho a disponer de los bienes se transfiere al sujeto pasivo contemplado en la letra c) de ese apartado, se aplicarán las normas siguientes:

a) se considerará que una entrega de bienes, exenta del IVA de conformidad con el artículo 138, apartado 1, ha sido realizada por el sujeto pasivo certificado que ha expedido o transportado los bienes, por sí mismo o por un tercero a su nombre, en el Estado miembro a partir del cual los bienes han sido expedidos o transportados;

b) se considerará que una adquisición intracomunitaria de bienes ha sido realizada por el sujeto pasivo al que se hace entrega de ellos en el Estado miembro al que se han expedido o transportado los bienes.».

3) En el artículo 138, el apartado 1 se sustituye por el texto siguiente:

«1. Los Estados miembros eximirán las entregas de bienes expedidos o transportados a un destino fuera de su respectivo territorio, pero dentro de la Comunidad, por el vendedor o en su nombre, o por el adquiriente de los bienes, cuando se cumplan las siguientes condiciones:

a) los bienes se entregan a otro sujeto pasivo, o a una persona jurídica no sujeta al impuesto, actuando en su condición de tal en un Estado miembro distinto de aquel en el que se inicia la expedición o el transporte de los bienes;

b) el sujeto pasivo, o la persona jurídica no sujeta al impuesto, a quien se hace entrega de los bienes está identificado a efectos del IVA en un Estado miembro distinto de aquel en el que se inicia la expedición o el transporte de los bienes;

c) en el estado recapitulativo presentado por el proveedor con arreglo al artículo 262, se hace referencia a la persona que adquiere los bienes.».

4) Se inserta el artículo 138 *bis* siguiente:

«Artículo 138 bis

1. A efectos de la aplicación de las exenciones previstas en el artículo 138 en el caso de operación en cadena, el transporte intracomunitario se imputará a la entrega al operador intermediario efectuada por el proveedor, cuando se cumplan las condiciones siguientes:

a) el operador intermediario comunica al proveedor el nombre del Estado miembro de llegada de los bienes;

b) el operador intermediario está identificado a efectos del IVA en un Estado miembro distinto de aquel en el que se inicia la expedición o el transporte de los bienes.

2. Cuando no se cumpla alguna de las condiciones establecidas en el apartado 1, en el caso de operación en cadena, el transporte intracomunitario se imputará a la entrega efectuada por el operador intermediario al cliente.

3. A los efectos del presente artículo, se entenderá por:

a) «caso de operación en cadena»: una situación en la que entregas sucesivas de los mismos bienes por sujetos pasivos dan lugar a un único transporte intracomunitario de dichos bienes, y en la que tanto el operador intermediario como el proveedor son sujetos pasivos certificados;

b) «operador intermediario»: un proveedor de la cadena distinto del primer proveedor, que expide o transporta los bienes, por sí mismo o por un tercero en su nombre;

c) «proveedor»: el sujeto pasivo de la cadena que entrega los bienes al operador intermediario;

d) «cliente»: el sujeto pasivo a quien el operador intermediario de la cadena entrega los bienes.».

5) En el artículo 243 se añade el apartado 3 siguiente:

«3. Todo sujeto pasivo certificado que transfiera bienes en el marco de los acuerdo de existencias de reserva a que se refiere el artículo 17 *bis* deberá llevar un registro de la siguiente información:

a) los bienes expedidos o transportados a otro Estado miembro y la dirección en la que son almacenados en ese Estado miembro;

b) los bienes entregados en una fase posterior y tras su llegada al Estado miembro a que se refiere la letra a).

Todo sujeto pasivo certificado al que se haga entrega de bienes en el marco de los acuerdos de existencias de reserva a que se refiere el artículo 17 *bis* deberá llevar un registro de dichos bienes.».

6) El artículo 262 se sustituye por el texto siguiente:

«Artículo 262

1. Los sujetos pasivos identificados a efectos del IVA deberán presentar un estado recapitulativo en el que figure la siguiente información:

a) los adquirientes identificados a efectos del IVA a quienes hayan entregado bienes en las condiciones previstas en el artículo 138, apartado 1 y apartado 2, letra c);

b) las personas identificadas a efectos del IVA a quienes hayan entregado bienes en el marco de las adquisiciones intracomunitarias contempladas en el artículo 42;

c) los sujetos pasivos y las personas jurídicas no sujetas al impuesto identificadas a efectos del IVA a quienes hayan prestado servicios que no estén exentos del IVA en el Estado miembro en el que la operación esté gravada, y respecto de los cuales el destinatario sea el deudor del impuesto, de conformidad con el artículo 196.».

2. Además de la información a que se refiere el apartado 1, cada sujeto pasivo certificado deberá identificar a los sujetos pasivos certificados a quienes están destinados los bienes expedidos o transportados en el marco de acuerdos de existencias de reserva en las condiciones establecidas en el artículo 17 *bis*.».

7) El título del capítulo 1 del título IV se sustituye por el siguiente:

«Régimen definitivo de tributación de los intercambios entre los Estados miembros»

El texto del artículo 402 se sustituye por el siguiente:

«Artículo 402

El régimen de tributación de los intercambios entre los Estados miembros establecido en la presente Directiva es transitorio y será sustituido por un régimen definitivo basado en los principios de tributación de las entregas de bienes y las prestaciones de servicios en el Estado miembro de destino; de sujeción al IVA del proveedor o del adquiriente en caso de que sea un sujeto pasivo certificado; y de un sistema de registro único para la declaración, liquidación y deducción del impuesto.».

9) Se suprimen los artículos 403 y 404.

Artículo 2

1. Los Estados miembros adoptarán y publicarán, a más tardar el 31 de diciembre de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

Aplicarán dichas disposiciones a partir del 1 de enero de 2019.

Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 3

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

Artículo 4

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Bruselas, el

Por el Consejo
El Presidente

COMISIÓN
EUROPEA

Bruselas, 4.10.2017
SWD(2017) 326 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

Propuesta de Directiva del Consejo

por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros

{COM(2017) 569 final}
{SWD(2017) 325 final}

Ficha resumen

Evaluación de impacto relativa a la Propuesta de Directiva del Consejo por la que se modifica la Directiva 2006/112/CE en lo que se refiere a la armonización y la simplificación de determinadas normas del régimen del impuesto sobre el valor añadido y se introduce el régimen definitivo de tributación de los intercambios entre los Estados miembros

A. Necesidad de actuar

¿Por qué? ¿Cuál es el problema que se afronta?

Las disposiciones transitorias de la Directiva sobre el IVA que regulan a las operaciones de bienes entre empresas dentro de la UE provocan: i) pérdidas de ingresos para los Estados miembros de alrededor de 50 000 millones EUR debido al fraude intracomunitario del operador desaparecido, surgido al amparo de las deficiencias endémicas del sistema, que permite la compra transfronteriza de bienes exentos de IVA; ii) una complejidad que hace que las empresas que se dedican al comercio transfronterizo tengan costes mayores que las empresas que operan solo a nivel nacional (un 11 % superiores) debido a las obligaciones adicionales que recaen en las primerasy a la aplicación divergente de las normas del IVA por parte de los Estados miembros. Sin una acción a escala de la UE, las posibles soluciones seguirían estando fragmentadas y tendrían unos beneficios limitados.

¿Cuál es el objetivo que se espera alcanzar con esta iniciativa?

Mediante unas disposiciones definitivas de imposición del comercio intracomunitario se pretende implantar en la UE un régimen del IVA más sólido, abordando sus deficiencias endémicas, y más simple, reduciendo sus complejidades, y establecer unas condiciones más equitativas para las empresas, independientemente de que operen a escala nacional o transfronteriza.

¿Cuál es el valor añadido de la actuación a nivel de la UE?

Para modificar las disposiciones transitorias, que ya no dan más de sí, se precisa una modificación de la Directiva sobre el IVA.

B. Soluciones

¿Qué opciones legislativas y no legislativas se han estudiado? ¿Existe o no una opción preferida? ¿Por qué?

- Opción 1: los clientes siguen realizando adquisiciones transfronterizas exentas del IVA, pero se introducen cambios en relación con determinadas operaciones (número a efectos del IVA y simplificaciones concedidas a los sujetos pasivos certificados[1]).
- Opción 2: los proveedores cobran el IVA en el Estado miembro al que llegan los bienes (excepto en el caso de los sujetos pasivos certificados). Una ventanilla única permite a las empresas pagar en su Estado miembro de origen el IVA adeudado en cualquier Estado miembro.
- Opción 3: cambio técnico equivalente al actual sistema (descartado).
- Opción 4: alineación con las normas sobre servicios.
- Opción 5: similar a la opción 2, pero la imposición tiene lugar en el Estado miembro en el que el cliente está establecido.

La opción 2 es la preferida (aborda tanto el problema del fraude como el problema de la complejidad), combinada con la opción 1 ,que permite una transición suave a la opción 2.

¿Quién apoya cada opción?

Los Estados miembros y las empresas apoyan la opción 1. Por otra parte, los Estados miembros también podrían apoyar la opción 2, y las empresas, las opciones 4 y 5.

C. Repercusiones de la opción preferida

¿Cuáles son las ventajas de la opción preferida (si existe, o bien de las principales opciones)?

Opción 2: Estados miembros: Reducción del fraude intracomunitario del operador desaparecido en 41 000 millones EUR.

[1] Un sujeto pasivo certificado es una empresa reconocida como «fiable» por las administraciones fiscales.

Empresas: Disminución de los costes de cumplimiento (1 000 millones EUR).

Mercado interior: Igualdad de trato de las entregas nacionales y transfronterizas de bienes y aumento neto de 18 500 millones EUR del PIB de la UE en un período de 3 años.

La opción 1 reduce los costes de cumplimiento para las empresas (500 millones EUR anuales).

Las repercusiones sociales y medioambientales no son significativas.

¿Cuáles son los costes de la opción preferida (si existe, o bien de las principales opciones)?

Opción 2: Estados miembros: aumento de los costes administrativos para los Estados miembros por un importe de 385 millones EUR en el año de aplicación y 311 millones en los años posteriores.

Empresas: Algunas pymes pueden experimentar un aumento del 6 % del coste anual de cumplimiento.

La opción 1 incrementa los costes administrativos para los Estados miembros por valor de 35 millones EUR y no consigue la igualdad de trato entre las entregas nacionales y transfronterizas de bienes.

Las repercusiones sociales y medioambientales no son significativas.

¿Cómo se verán afectadas las empresas, las pymes y las microempresas?

La iniciativa no prevé un trato preferente para las pymes. Aborda los problemas de todas las empresas. Las microempresas seguirán beneficiándose del régimen de exención del IVA y de las nuevas medidas de simplificación específicamente destinadas a ellas contenidas en el próximo paquete de simplificación para las pymes[2].

¿Habrá repercusiones significativas en los presupuestos y las administraciones nacionales?

A escala de la UE, se prevé un beneficio neto de unos 43 000 millones EUR gracias a la reducción de la incidencia del fraude intracomunitario del operador desaparecido y a la incidencia de los flujos de caja, que compensarían con creces el aumento de los costes administrativos.

¿Habrá otras repercusiones significativas?

La transición al nuevo régimen obliga a los Estados miembros y a las empresas a adaptarse a las nuevas normas (aplicación + control).

D. Seguimiento

¿Cuándo se revisará la política?

Aplicación gradual:
Primera Directiva (septiembre de 2017): aplicación de la opción 1 («soluciones rápidas» asociadas al estatuto de sujeto pasivo certificado) e introducción de los pilares de la opción 2.
Segunda Directiva (2018): plena aplicación de la opción 2.
Seguimiento (por ejemplo, número de sujetos pasivos certificados o problemas de aplicación) a través del Comité del IVA, el Grupo sobre el futuro del IVA y el Grupo de expertos sobre el IVA.
Evaluación: cinco años después de la entrada en vigor de la segunda Directiva.

[2] Plan de Acción de la Comisión [COM(2016) 148 final].

BOLETÍN OFICIAL DO

XXX lexislatura

Número XXX

Fascículo XX

PARLAMENTO DE GALICIA

BOLETÍN OFICIAL DO
PARLAMENTO DE GALICIA

Edición e subscricións:
Servizo de Publicacións do Parlamento de Galicia. Hórreo, 63. 15702. Santiago de Compostela.
Telf. 981 55 13 00. Fax. 981 55 14 25
Dep. Leg. C-155-1982. ISSN 1133-2727