Diario Oficial de la Unión Europea

L 151

Edición en lengua española

Legislación

62.° año

7 de junio de 2019

Sumario

[1] Texto pertinente a efectos del EEE.

ES

Los actos cuyos títulos van impresos en caracteres finos son actos de gestión corriente, adoptados en el marco de la política agraria, y que tienen generalmente un período de validez limitado.

Los actos cuyos títulos van impresos en caracteres gruesos y precedidos de un asterisco son todos los demás actos.

I

(Actos legislativos)

REGLAMENTOS

REGLAMENTO(UE) 2019/880 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

relativo a la introducción y la importación de bienes culturales

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 207, apartado 2,

Vista la propuesta de la Comisión Europea,

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

De conformidad con el procedimiento legislativo ordinario ([1]),

Considerando lo siguiente:

(1) Vistas las Conclusiones del Consejo de 12 de febrero de 2016 sobre la lucha contra la financiación del terrorismo, la Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 2 de febrero de 2016, relativa a un plan de acción para intensificar la lucha contra la financiación del terrorismo y la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo ([2]), deben adoptarse normas comunes sobre el comercio con terceros países a fin de garantizar la protección eficaz contra el comercio ilícito de bienes culturales, así como contra su pérdida o destrucción, la conservación del patrimonio cultural de la humanidad y la prevención de la financiación del terrorismo y el blanqueo de capitales a través de la venta a compradores en la Unión de bienes culturales saqueados.

(2) La explotación de pueblos y territorios puede conducir al comercio ilícito de bienes culturales, en particular cuando el comercio ilícito tiene su origen en un contexto de conflicto armado. A este respecto, el presente Reglamento debe tener en cuenta las particularidades regionales y locales de los pueblos y territorios, en lugar del valor de mercado de los bienes culturales.

(3) Los bienes culturales que son parte del patrimonio cultural revisten con frecuencia una gran importancia desde el punto de vista cultural, artístico, histórico y científico. El patrimonio cultural constituye uno de los elementos básicos de la civilización, entre otras cosas, por su valor simbólico y por formar parte de la memoria cultural de la humanidad. Enriquece la vida cultural de todos los pueblos y une a las personas a través de la memoria compartida, el conocimiento y el desarrollo de la civilización. Debe por tanto gozar de protección contra la apropiación ilícita y el saqueo. Siempre ha habido saqueos de yacimientos arqueológicos, pero actualmente se produce a escala industrial y constituye, junto con el comercio de bienes culturales excavados ilícitamente, un delito grave que provoca mucho sufrimiento a las personas afectadas directa o indirectamente. El comercio ilícito de bienes culturales contribuye en muchos casos a una homogeneización cultural forzosa o a la pérdida forzosa de la identidad cultural, mientras que el saqueo de bienes culturales conduce, entre otras cosas, a la desintegración de las culturas. Mientras sea posible participar en un comercio lucrativo de bienes culturales excavados ilícitamente y obtener beneficios de dicho comercio sin grandes riesgos, tales excavaciones y saqueos seguirán produciéndose. Debido a su valor económico y artístico, los bienes culturales s acusan una fuerte demanda en el mercado internacional. La ausencia de medidas jurídicas internacionales firmes y la ineficaz aplicación de las medidas existentes dan lugar a que estos bienes pasen a la economía sumergida. En consecuencia, la Unión debe prohibir la introducción en su territorio aduanero de bienes culturales exportados ilícitamente desde terceros países, prestando especial atención a los bienes culturales procedentes de terceros países afectados por conflictos armados, en particular cuando dichos bienes culturales hayan sido objeto de comercio ilícito por parte de organizaciones

([1]) Posición del Parlamento Europeo de 12 de marzo de 2019 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.

([2]) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

terroristas u otro tipo de organizaciones criminales. Si bien esta prohibición general no ha de conllevar controles sistemáticos, los Estados miembros han de poder intervenir cuando reciban información sobre envíos sospechosos y tomar todas las medidas adecuadas para interceptar bienes culturales exportados ilícitamente.

(4) Habida cuenta de que los distintos Estados miembros aplican normas diferentes sobre la importación de bienes culturales en el territorio aduanero de la Unión, deben tomarse medidas para, en particular, garantizar que determinadas importaciones de bienes culturales sean sometidas a controles uniformes en el momento de su entrada en el territorio aduanero de la Unión, sobre la base de los procesos, procedimientos e instrumentos administrativos existentes destinados a conseguir una aplicación uniforme del Reglamento (UE) n.º 952/2013 del Parlamento Europeo y del Consejo ([3]).

(5) La protección de los bienes culturales considerados patrimonio nacional de los Estados miembros ya está contemplada en el Reglamento (CE) n.º 116/2009 del Consejo ([4]) y en la Directiva 2014/60/UE del Parlamento Europeo y del Consejo ([5]). Por tanto, el presente Reglamento no debe aplicarse a los bienes culturales que hayan sido creados o descubiertos en el territorio aduanero de la Unión. Las normas comunes introducidas por el presente Reglamento deben abarcar el tratamiento aduanero de los bienes culturales que, no procediendo de la Unión, entren en su territorio aduanero. A efectos de la aplicación del presente Reglamento, el territorio aduanero pertinente debe ser el territorio aduanero de la Unión en el momento de la importación.

(6) Las medidas de control que deben establecerse en relación con las zonas francas y los llamados «puertos francos» han de tener un ámbito de aplicación lo más amplio posible en cuanto a los procedimientos aduaneros correspondientes, a fin de impedir la elusión del presente Reglamento mediante la explotación de dichas zonas francas, con potencial para ser utilizadas para la proliferación continuada del comercio ilícito. Por tanto, dichas medidas de control no deben afectar únicamente a los bienes culturales despachados a libre práctica, sino también a los bienes culturales incluidos en regímenes aduaneros especiales. Sin embargo, su alcance no debe ir más allá d del objetivo consistente en impedir que los bienes culturales exportados ilícitamente entren en el territorio aduanero de la Unión. Por consiguiente, aunque han de abarcar el despacho a libre práctica y algunos de los regímenes aduaneros especiales en que pueden incluirse los bienes que entran en el territorio aduanero de la Unión, las medidas de control sistemático deben excluir el tránsito.

(7) Muchos terceros países y la mayoría de los Estados miembros están familiarizados con las definiciones que se utilizan en la Convención de la UNESCO sobre las medidas que deben adoptarse para prohibir e impedir la importación, la exportación y la transferencia de propiedad ilícitas de bienes culturales, firmada en París el 14 de noviembre de 1970 (en lo sucesivo, «Convención de la UNESCO de 1970»), en la que son parte un número importante de Estados miembros, y en el Convenio del UNIDROIT sobre los bienes culturales robados o exportados ilícitamente, firmado en Roma el 24 de junio de 1995. Por esta razón, las definiciones utilizadas en el presente Reglamento se basan en dichas definiciones.

(8) La legalidad de la exportación de bienes culturales debe examinarse principalmente en función de las disposiciones legales y reglamentarias del país en que se hayan creado o descubierto esos bienes culturales. No obstante, para no obstaculizar de forma injustificada el comercio legítimo, se debe, en determinados casos, permitir excepcionalmente a la persona que desea importar bienes culturales en el territorio aduanero de la Unión demostrar, en su lugar, la legalidad de la exportación desde un tercer país diferente en el que se encontraban los bienes culturales antes de su envío al territorio de la Unión. Esa excepción debe aplicarse cuando no pueda determinarse con fiabilidad en qué país se crearon o descubrieron los bienes culturales, o cuando la exportación de los bienes culturales en cuestión haya ocurrido antes de que entrase en vigor la Convención de la UNESCO de 1970, es decir, el 24 de abril de 1972. Con el fin de impedir que se eluda el cumplimiento del presente Reglamento simplemente enviando bienes culturales exportados ilícitamente a otro tercer país antes de importarlos en la Unión, las excepciones han de aplicarse si los bienes culturales estuvieron en un tercer país por un período de tiempo superior a cinco años con fines distintos del uso temporal, el tránsito, la reexportación o el transbordo. Si tales condiciones se cumplen para más de un país, el país de que se trata debe ser el último de dichos países con anterioridad a la introducción de los bienes culturales en el territorio aduanero de la Unión.

(9) El artículo 5 de la Convención de la UNESCO de 1970 insta a los Estados Partes a crear uno o varios servicios nacionales para la protección de los bienes culturales contra la importación, la exportación y la transferencia de propiedad ilícitas. Dichos servicios nacionales deben estar dotados de personal competente y en número suficiente que garantice esa protección de conformidad con la citada Convención, y deben además posibilitar la colaboración activa necesaria entre las autoridades competentes de los Estados miembros que son partes en la Convención en el ámbito de la seguridad y en la lucha contra la importación ilícita de bienes culturales, especialmente de zonas afectadas por conflictos armados.

([3]) Reglamento (UE) n.º 952/2013 del Parlamento Europeo y del Consejo, de 9 de octubre de 2013, por el que se establece el código aduanero de la Unión (DO L 269 de 10.10.2013, p. 1).

([4]) Reglamento (CE) n.º 116/2009 del Consejo, de 18 de diciembre de 2008, relativo a la exportación de bienes culturales (DO L 39 de 10.2.2009, p. 1).

([5]) Directiva 2014/60/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la restitución de bienes culturales que hayan salido de forma ilegal del territorio de un Estado miembro, y por la que se modifica el Reglamento (UE) n.º 1024/2012 (DO L 159 de 28.5.2014, p. 1).

(10) A fin de no obstaculizar de manera desproporcionada el comercio de bienes culturales a través de las fronteras exteriores de la Unión, el presente Reglamento debe aplicarse únicamente a los bienes culturales que superen un determinado límite de antigüedad, tal como se establece en el presente Reglamento. También parece conveniente fijar un umbral financiero con el fin de que los bienes culturales de valor inferior queden excluidos de la aplicación de las condiciones y los procedimientos establecidos para la importación en el territorio aduanero de la Unión. Tales umbrales garantizarán que las medidas establecidas en el presente Reglamento se centren en aquellos bienes culturales más propensos al saqueo en zonas de conflicto, sin excluir otros bienes cuyo control es necesario para garantizar la protección del patrimonio cultural.

(11) En el contexto de la evaluación supranacional de los riesgos en materia de blanqueo de capitales y financiación del terrorismo que afectan al mercado interior, se ha detectado que el comercio ilícito de bienes culturales saqueados puede ser una fuente de financiación del terrorismo y del blanqueo de capitales.

(12) Dado que determinadas categorías de bienes culturales, a saber, los objetos arqueológicos y los elementos de monumentos son particularmente vulnerables al saqueo y la destrucción, es necesario establecer un sistema de control reforzado antes de que estén autorizados a entrar en el territorio aduanero de la Unión. Tal sistema debe exigir la presentación de una licencia de importación expedida por la administración competente de un Estado miembro con anterioridad al despacho a libre práctica de tales bienes culturales en la Unión o de su inclusión en un régimen aduanero especial distinto del de tránsito. Las personas que deseen obtener dicha licencia deben acreditar la exportación lícita desde el país en el que se crearon o descubrieron los bienes culturales con documentos justificativos y pruebas adecuados, como certificados de exportación, títulos de propiedad, facturas, contratos de compraventa, documentos de seguros, documentos de transporte y peritajes. Las autoridades de los Estados miembros deben decidir, sobre la base de solicitudes completas y precisas, si expedir o no una licencia sin demora indebida. Toda licencia de importación debe archivarse en un sistema electrónico.

(13) Se entiende por imagen religiosa toda representación de una figura o un acontecimiento religioso. Puede ser elaborada en diferentes materiales y tamaños, ser de naturaleza monumental o portátil. Una imagen religiosa que algún momento hayan formado parte, por ejemplo, del interior de una iglesia, monasterio, capilla, ya sea en una pieza separada o integrada en el mobiliario arquitectónico, por ejemplo un iconostasio o soporte para imágenes, es una parte esencial e inseparable del culto y la vida litúrgica, y debe considerarse elemento integral de un monumento religioso que haya sido desmembrado. Incluso cuando el monumento concreto al que pertenezca la imagen religiosa sea desconocido, pero haya pruebas de que dicha imagen fue en algún momento un elemento integral de un monumento, en particular cuando presente signos o elementos que indiquen que formó parte en algún momento de un iconostasio o un soporte para imágenes, la imagen religiosa aún debe estar incluida en la categoría de «elementos procedentes de la desmembración de monumentos artísticos o históricos o de lugares de interés arqueológico» enumerada en el anexo.

(14) Habida cuenta de la naturaleza específica de los bienes culturales, las autoridades aduaneras desempeñan una función sumamente importante y deben tener la posibilidad, en caso necesario, de exigir información adicional al declarante y analizar los bienes culturales mediante la realización de un examen físico.

(15) En el caso de las categorías de bienes culturales que no requieren una licencia de importación, las personas que deseen importar tales bienes en el territorio aduanero de la Unión deben certificar, mediante una declaración, que la exportación desde el tercer país es legal y asumir la responsabilidad correspondiente, además de proporcionar información suficiente para que los bienes culturales en cuestión puedan ser identificados por las autoridades aduaneras. A fin de facilitar el procedimiento y por motivos de seguridad jurídica, la información sobre el bien cultural debe aportarse empleando un documento normalizado. Para describir los bienes culturales podría utilizarse el formulario de identificación de objetos recomendado por la UNESCO. El titular de las mercancías debe registrar esos datos en un sistema electrónico para facilitar la identificación por las autoridades aduaneras, permitir la realización de análisis de riesgos y controles específicos y garantizar la trazabilidad una vez que los bienes culturales entren en el mercado interior.

(16) En el contexto del entorno de ventanilla única de la Unión para las aduanas, la Comisión debe ser responsable de establecer un sistema electrónico centralizado para la presentación de las solicitudes de licencias de importación y de las declaraciones del importador, así como para el almacenamiento y el intercambio de información entre las autoridades de los Estados miembros, en particular en lo relativo a las declaraciones del importador y las licencias de importación.

(17) El tratamiento de datos en virtud del presente Reglamento también ha de poder abarcar los datos personales y ha de llevarse a cabo de conformidad con el Derecho de la Unión. Los Estados miembros y la Comisión deben tratar los datos personales exclusivamente para los fines del presente Reglamento o, en circunstancias debidamente justificadas, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Toda recogida, revelación, transmisión, comunicación u otro tratamiento de datos personales dentro del

ámbito de aplicación del presente Reglamento debe estar sujeto a los requisitos de los Reglamentos (UE) 2016/679 ([6]) y (UE) 2018/1725 ([7]) del Parlamento Europeo y del Consejo. El tratamiento de datos personales a efectos del presente Reglamento también debe respetar el derecho al respeto de la vida privada y familiar reconocido por el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales del Consejo de Europa, así como el derecho al respeto de la vida privada y familiar y el derecho a la protección de datos de carácter personal reconocidos por los artículos 7 y 8, respectivamente, de la Carta de los Derechos Fundamentales de la Unión Europea.

(18) Los bienes culturales que no se hayan creado ni descubierto en el territorio aduanero de la Unión pero que se hayan exportado como mercancías de la Unión no deben estar sujetos a la presentación de una licencia de importación ni de una declaración del importador cuando se devuelvan a ese territorio como mercancías de retorno en el sentido del Reglamento (UE) n.º 952/2013.

(19) La importación temporal de bienes culturales con fines educativos, científicos, de conservación, restauración, exposición, digitalización, artes escénicas, investigación por parte de instituciones educativas o cooperación entre museos o entidades similares tampoco debe estar sujeta a la presentación de una licencia de importación o de una declaración del importador.

(20) El depósito de bienes culturales provenientes de países afectados por conflictos armados o catástrofes naturales con la finalidad exclusiva de garantizar su custodia y conservación o supervisión por parte de una autoridad pública no debe estar sujeto a la presentación de una licencia de importación o de una declaración del importador.

(21) Para facilitar la presentación de bienes culturales en ferias de arte comerciales, no debe ser necesaria la licencia de importación en los casos en que los bienes culturales estén sujetos a importación temporal en el sentido del artículo 250 del Reglamento (UE) n.º 952/2013, y se haya aportado una declaración del importador en lugar de la licencia de importación. No obstante, debe exigirse la presentación de una licencia de importación cuando esos bienes culturales vayan a permanecer en la Unión al término de la feria de arte.

(22) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para adoptar disposiciones pormenorizadas con respecto a los bienes culturales que sean bienes de retorno o la importación temporal de bienes culturales en el territorio aduanero de la Unión y su custodia, los modelos para las solicitudes de licencias de importación y los formularios de las licencias de importación, los modelos para las declaraciones del importador y su documentación adjunta, y las normas de procedimiento complementarias sobre su presentación y tratamiento. También deben conferirse a la Comisión competencias de ejecución que le permitan tomar medidas con el fin de establecer un sistema electrónico para la presentación de solicitudes de licencias de importación y declaraciones del importador y para el almacenamiento e intercambio de información entre Estados miembros. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([8]).

(23) Para garantizar una coordinación efectiva y evitar la duplicación de esfuerzos al organizar actividades de formación y capacitación y campañas de sensibilización, así como para encargar investigaciones pertinentes y la elaboración de normas, cuando proceda, la Comisión y los Estados miembros deben colaborar con organizaciones y organismos internacionales como UNESCO, Interpol, Europol, la Organización Mundial de Aduanas, el Centro Internacional de Estudio para la Conservación y la Restauración de los Bienes Culturales y el Consejo Internacional de Museos.

(24) A fin de respaldar la aplicación eficiente del presente Reglamento y aportar una base para su futura evaluación, los Estados miembros y la Comisión deben recopilar y compartir por vía electrónica información pertinente sobre los flujos comerciales de bienes culturales. En aras de la transparencia y el examen público, debe hacerse pública tanta información como sea posible. El flujo comercial de bienes culturales no se puede controlar de manera eficiente en función únicamente de su valor o peso. Es fundamental reunir información por vía electrónica sobre el número de artículos declarados. Dado que en la nomenclatura combinada no se especifica medición complementaria alguna para los bienes culturales, es necesario exigir la declaración del número de artículos.

([6]) 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).

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

([8]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(25) La Estrategia y el Plan de Acción de la UE para la Gestión de los Riesgos Aduaneros pretende, entre otras cosas, reforzar las capacidades de las autoridades aduaneras para aumentar la respuesta frente a los riesgos en el ámbito de los bienes culturales. Debe utilizarse el marco común de gestión de riesgos establecido en el Reglamento (UE) n.º 952/2013 y las autoridades aduaneras han de intercambiar la información pertinente sobre el riesgo.

(26) Para aprovechar los conocimientos especializados de las organizaciones y organismos internacionales que son activos en asuntos culturales y su experiencia con el comercio ilícito de bienes culturales, deben tenerse en cuenta en el marco común de gestión de riesgos las recomendaciones y orientaciones procedentes de esos organismos y organizaciones a la hora de detectar riesgos relacionados con bienes culturales. En particular, las listas rojas publicadas por el Consejo Internacional de Museos deben servir de orientación para determinar los terceros países cuyo patrimonio corre mayor riesgo y los objetos exportados desde esos países que con mayor frecuencia son objeto de comercio ilícito.

(27) Es necesario realizar campañas de sensibilización dirigidas a compradores de bienes culturales sobre el riesgo derivado del comercio ilícito y ayudar a los operadores del mercado a comprender y aplicar el presente Reglamento. Los Estados miembros deben implicar a los puntos de contacto nacionales pertinentes y otros servicios de información para difundir dicha información.

(28) La Comisión debe velar por que las microempresas y las pequeñas y medianas empresas (pymes) disfruten de una asistencia técnica adecuada y debe facilitar el suministro de información a dichas empresas, a fin de aplicar de forma eficiente el presente Reglamento. Las pymes establecidas en la Unión que importen bienes culturales deben, por tanto, beneficiarse de los programas actuales y futuros de la Unión que favorezcan su competitividad.

(29) Con objeto de fomentar el cumplimiento e impedir la elusión, los Estados miembros deben introducir sanciones efectivas, proporcionadas y disuasorias para los casos de incumplimiento de las disposiciones del presente Reglamento y comunicar dichas sanciones a la Comisión. Las sanciones introducidas por los Estados miembros por las infracciones del presente Reglamento deben tener un efecto disuasorio equivalente en toda la Unión.

(30) Los Estados miembros deben garantizar que las autoridades aduaneras y las autoridades competentes acuerden medidas en virtud del artículo 198 del Reglamento (UE) n.º 952/2013. Los pormenores de dichas medidas deben regirse por el Derecho nacional.

(31) La Comisión debe adoptar sin demora normas de ejecución del presente Reglamento, especialmente las relativas a los formularios electrónicos normalizados apropiados que han de utilizarse para la solicitud de licencias de importación o para la preparación de una declaración del importador, y establecer posteriormente el sistema electrónico en el plazo más breve posible. La aplicación de las disposiciones relativas a las licencias de importación y las declaraciones del importador debe aplazarse en consecuencia.

(32) De acuerdo con el principio de proporcionalidad, es necesario y conveniente para alcanzar los objetivos fundamentales del presente Reglamento regular las normas sobre la introducción, y las condiciones y procedimientos para la importación de bienes culturales en el territorio aduanero de la Unión. El presente Reglamento no excede de lo necesario para alcanzar los objetivos perseguidos, de conformidad con lo dispuesto en el artículo 5, apartado 4, del Tratado de la Unión Europea.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto y ámbito de aplicación

1. El presente Reglamento establece las condiciones para la introducción de bienes culturales y las condiciones y procedimientos para la importación de bienes culturales con fines de salvaguardia del patrimonio cultural de la humanidad y de prevención del comercio ilícito de bienes culturales, en particular en los casos en los que dicho comercio ilícito pueda contribuir a la financiación del terrorismo.

2. El presente Reglamento no se aplicará a los bienes culturales que se hayan creado o descubierto en el territorio aduanero de la Unión.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «bienes culturales»: cualquier artículo que revista importancia para la arqueología, la prehistoria, la historia, la literatura, el arte o la ciencia, enumerado en el anexo;

2) «introducción de bienes culturales»: toda entrada de bienes culturales en el territorio aduanero de la Unión que esté sujeta a vigilancia aduanera o control aduanero en el territorio aduanero de la Unión de conformidad con el Reglamento (UE) n.º 952/2013;

3) «importación de bienes culturales»:

a) el despacho de bienes culturales a libre práctica a que se refiere el artículo 201 del Reglamento (UE) n.º 952/2013, o

b) la inclusión de bienes culturales en una de las siguientes categorías de regímenes especiales contempladas en el artículo 210 del Reglamento (UE) n.º 952/2013:

i) el depósito, incluidos el depósito aduanero y las zonas francas,

ii) los destinos especiales, incluidos la importación temporal y el destino final,

iii) el perfeccionamiento activo;

4) «titular de las mercancías»: el titular de las mercancías según se define en el artículo 5, punto 34, del Reglamento (UE) n.º 952/2013;

5) «autoridades competentes»: las autoridades públicas designadas por los Estados miembros para expedir licencias de importación.

Artículo 3

Introducción e importación de bienes culturales

1. Queda prohibida la introducción de los bienes culturales mencionados en la parte A del anexo que hayan salido del territorio del país en el que se crearon o descubrieron en infracción de las disposiciones legales y reglamentarias de dicho país.

Las autoridades aduaneras y las autoridades competentes tomarán cualquier medida adecuada cuando se produzca un intento de introducir los bienes culturales a que se refiere el párrafo primero.

2. La importación de los bienes culturales enumerados en las partes B y C del anexo se permitirá únicamente previa presentación de:

a) una licencia de importación expedida de conformidad con el artículo 4, o

b) una declaración del importador presentada de conformidad con el artículo 5.

3. La licencia de importación o la declaración del importador a que se refiere el apartado 2 del presente artículo se facilitarán a las autoridades aduaneras de conformidad con el artículo 163 del Reglamento (UE) n.º 952/2013. En caso de inclusión de bienes culturales en el régimen de zona franca, el titular de las mercancías facilitará la licencia de importación o la declaración del importador en el momento de la presentación de los bienes de conformidad con lo dispuesto en el artículo 245, apartado 1, letras a) y b), del Reglamento (UE) n.º 952/2013.

4. El apartado 2 del presente artículo no se aplicará a:

a) los bienes culturales que sean bienes de retorno en el sentido del artículo 203 del Reglamento (UE) n.º 952/2013;

b) la importación de bienes culturales con la finalidad exclusiva de garantizar su custodia o supervisión por parte de una autoridad pública, con la intención de devolverlos cuando la situación lo permita;

c) la importación temporal de bienes culturales en el sentido del artículo 250 del Reglamento (UE) n.º 952/2013, en el territorio aduanero de la Unión con fines educativos, científicos, de conservación, restauración, exposición, digitalización, artes escénicas, investigación por parte de instituciones educativas o cooperación entre museos o entidades similares.

5. No se exigirá una licencia de importación para los bienes culturales a los que se ha aplicado el régimen de importación temporal en el sentido del artículo 250 del Reglamento (UE) n.º 952/2013 en caso de que dichos bienes vayan a presentarse en ferias de arte comerciales. Se facilitará en tales casos una declaración del importador de conformidad con el artículo 5 del presente Reglamento.

No obstante, si dichos bienes culturales se incluyen posteriormente en otro régimen aduanero contemplado en el artículo 2, punto 3, del presente Reglamento, se requerirá licencia de importación expedida de conformidad con el su artículo 4.

6. La Comisión establecerá, mediante actos de ejecución, disposiciones pormenorizadas en lo que respecta a los bienes culturales que sean bienes de retorno, a la importación de bienes culturales para su custodia y a la importación temporal de bienes culturales a que se refieren los apartados 4 y 5 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 13, apartado 2.

7. El apartado 2 del presente artículo se entenderá sin perjuicio de otras medidas adoptadas por la Unión de conformidad con el artículo 215 del Tratado de Funcionamiento de la Unión Europea.

8. Al presentar una declaración aduanera para la importación de bienes culturales enumerados en las partes B y C del anexo, el número de artículos se indicará utilizando la unidad suplementaria como establece el anexo. En caso de inclusión de los bienes culturales en el régimen de zona franca, el titular de las mercancías indicará el número de artículos en el momento de la presentación de los bienes de conformidad con el artículo 245, apartado 1, letras a) y b), del Reglamento (UE) n.º 952/2013.

Artículo 4

Licencia de importación

1. La importación de bienes culturales enumerados en la parte B del anexo distintos de los mencionados en el artículo 3, apartados 4 y 5, requerirá licencia de importación. Dicha licencia de importación será expedida por la autoridad competente del Estado miembro en el que los bienes culturales se incluyan por primera vez en uno de los regímenes aduaneros a los que se refiere el artículo 2, punto 3.

2. Las licencias de importación expedidas por las autoridades competentes de un Estado miembro de conformidad con lo dispuesto en el presente artículo serán válidas en toda la Unión.

3. Una licencia de importación expedida de conformidad con el presente artículo no se considerará prueba de procedencia o titularidad lícitas de los bienes culturales de que se trate.

4. El titular de las mercancías solicitará una licencia de importación a la autoridad competente del Estado miembro a que se refiere el apartado 1 del presente artículo a través del sistema electrónico a que se refiere el artículo 8. La solicitud deberá ir acompañada de cualesquiera documentos justificativos e información que demuestren que los bienes culturales de que se trate se exportaron desde el país en el que se crearon o descubrieron con arreglo a las disposiciones legales y reglamentarias de dicho país, o que demuestren la ausencia de tales disposiciones en el momento en el que salieron de su territorio.

No obstante lo dispuesto en el párrafo primero, la solicitud podrá, en su lugar, ir acompañada de cualesquiera documentos justificativos e información que demuestren que los bienes culturales de que se trate se exportaron de conformidad con las disposiciones legales y reglamentarias del último país en el que se hayan albergado durante un período superior a cinco años y con fines distintos del uso temporal, el tránsito, la reexportación o el transbordo, en los casos siguientes:

a) cuando el país en el que se crearon o descubrieron los bienes culturales no pueda determinarse con fiabilidad, o

b) cuando los bienes culturales hayan salido del país en el que se crearon o descubrieron antes del 24 de abril de 1972.

5. Las pruebas de que los bienes culturales de que se trate se exportaron de conformidad con el apartado 4 se aportarán en forma de certificados de exportación o licencias de exportación cuando el país de que se trate haya establecido tales documentos para la exportación de los bienes culturales en el momento de la exportación.

6. La autoridad competente comprobará que la solicitud esté completa. Pedirá al solicitante toda la información o documentos que falten o adicionales en un plazo de 21 días desde la recepción de la solicitud.

7. En un plazo de 90 días desde la recepción de la solicitud completa, la autoridad competente la examinará y decidirá si expide la licencia de importación o deniega la solicitud.

La autoridad competente denegará la solicitud cuando:

a) tenga información o motivos razonables para creer que los bienes culturales salieron del territorio del país en el que se crearon o descubrieron en infracción de las disposiciones legales y reglamentarias de dicho país;

b) no se hayan aportado las pruebas exigidas por el apartado 4;

c) tenga información o motivos razonables para creer que el titular de las mercancías no las adquirió legalmente, o

d) haya sido informada de la existencia de reclamaciones pendientes de devolución de los bienes culturales interpuestas por las autoridades del país en el que se crearon o descubrieron.

8. En caso de que la solicitud sea denegada, se notificará sin demora al solicitante la decisión administrativa a que se refiere el apartado 7, junto con una motivación e información sobre el procedimiento de recurso.

9. Cuando se presente una solicitud de licencia de importación relativa a bienes culturales para los que anteriormente se hubiera denegado una solicitud, el solicitante informará de la anterior denegación a la autoridad competente a la que presente la solicitud.

10. Cuando un Estado miembro deniegue una solicitud, la denegación y los motivos en que se basa se comunicarán a los demás Estados miembros y a la Comisión a través del sistema electrónico a que se refiere el artículo 8.

11. Los Estados miembros designarán sin demora a las autoridades competentes para la expedición de licencias de importación con arreglo al presente artículo. Los Estados miembros comunicarán a la Comisión los datos de dichas autoridades competentes y los cambios a este respecto.

La Comisión publicará los datos de las autoridades competentes y los cambios que les afecten en la serie C del *Diario Oficial de la Unión Europea*.

12. La Comisión establecerá, mediante actos de ejecución, el modelo y el formato de las solicitudes de licencia de importación, e indicará los posibles documentos justificativos que demuestren la procedencia lícita de los bienes culturales de que se trate, así como las normas de procedimiento sobre la presentación y tramitación de tales solicitudes. Al establecer esos elementos, la Comisión procurará lograr una aplicación uniforme por parte de las autoridades competentes de los procedimientos de expedición de licencias de importación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 13, apartado 2.

Artículo 5

Declaración del importador

1. La importación de los bienes culturales enumerados en la parte C del anexo requerirá una declaración del importador, que el titular de las mercancías presentará a través del sistema electrónico a que se refiere el artículo 8.

2. La declaración del importador constará de:

a) una declaración firmada por el titular de las mercancías en la que se haga constar que los bienes culturales se exportaron desde el país en el que se crearon o descubrieron con arreglo a las disposiciones legales y reglamentarias de dicho país en el momento en que salieron de su territorio, y

b) un documento normalizado que describa los bienes culturales en cuestión de forma suficientemente detallada para que puedan ser identificados por las autoridades y para llevar a cabo análisis de riesgos y controles específicos.

No obstante lo dispuesto en la letra a) del párrafo primero, la declaración podrá indicar en su lugar que los bienes culturales en cuestión se exportaron de conformidad con las disposiciones legales y reglamentarias del último país en el que se hayan albergado durante un período superior a cinco años y con fines distintos del uso temporal, el tránsito, la reexportación o el transbordo, en los casos siguientes:

a) cuando el país en el que se crearon o descubrieron los bienes culturales no pueda determinarse con fiabilidad, o

b) cuando los bienes culturales hayan salido del país en el que se crearon o descubrieron antes del 24 de abril de 1972.

3. La Comisión establecerá, mediante actos de ejecución, el modelo normalizado y el formato de la declaración del importador, así como las normas de procedimiento sobre su presentación, e indicará los posibles documentos justificativos para probar la procedencia lícita de los bienes culturales de que se trate que deben estar en posesión del titular de las mercancías y las normas sobre la tramitación de tal declaración. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 13, apartado 2.

Artículo 6

Aduanas competentes

Los Estados miembros podrán limitar el número de aduanas facultadas para tramitar la importación de bienes culturales a los que se aplica el presente Reglamento. Cuando los Estados miembros apliquen tal limitación, comunicarán a la Comisión los datos de estas aduanas y los cambios a este respecto.

La Comisión publicará los datos de dichas aduanas competentes y los cambios que les afecten en la serie C del *Diario Oficial de la Unión Europea*.

Artículo 7

Cooperación administrativa

A efectos de la aplicación del presente Reglamento, los Estados miembros velarán por la cooperación entre sus autoridades aduaneras y las autoridades competentes a las que se refiere el artículo 4.

Artículo 8

Utilización de un sistema electrónico

1. El almacenamiento y el intercambio de información entre las autoridades de los Estados miembros, en particular en lo que respecta a las licencias de importación y las declaraciones del importador, se llevará a cabo por medio de un sistema electrónico centralizado.

En caso de fallo temporal del sistema electrónico podrán utilizarse temporalmente otros medios de almacenamiento e intercambio de información.

2. La Comisión establecerá, mediante actos de ejecución:

a) las disposiciones para la creación, el funcionamiento y el mantenimiento del sistema electrónico a que se refiere el apartado 1;

b) las normas detalladas relativas a la presentación, la tramitación, el almacenamiento y el intercambio de información entre las autoridades de los Estados miembros a través del sistema electrónico o por otros medios a que se refiere el apartado 1.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 13, apartado 2, a más tardar el 28 de junio de 2021.

Artículo 9

Establecimiento de un sistema electrónico

La Comisión establecerá el sistema electrónico a que se refiere el artículo 8. El sistema electrónico estará operativo a más tardar cuatro años después de la entrada en vigor del primero de los actos de ejecución a que se refiere el artículo 8, apartado 2.

Artículo 10

Protección de datos personales y períodos de conservación de los datos

1. Las autoridades aduaneras y las autoridades competentes de los Estados miembros actuarán como responsables del tratamiento de los datos personales obtenidos de conformidad con los artículos 4, 5 y 8.

2. El tratamiento de los datos personales sobre la base del presente Reglamento se realizará únicamente para los fines definidos en el artículo 1, apartado 1.

3. Únicamente el personal debidamente autorizado de las autoridades podrá acceder a los datos personales obtenidos de conformidad con los artículos 4, 5 y 8, los cuales estarán convenientemente protegidos contra el acceso o la comunicación no autorizados. Los datos no podrán ser revelados o comunicados sin la autorización expresa y por escrito de la autoridad que haya obtenido inicialmente la información. No obstante, dicha autorización no será necesaria cuando las autoridades estén obligadas a revelar o comunicar dicha información con arreglo a las disposiciones legales vigentes en el Estado miembro de que se trate, en particular en el marco de un procedimiento judicial.

4. Las autoridades conservarán los datos personales obtenidos en aplicación de los artículos 4, 5 y 8 durante un período de veinte años a partir de la fecha de su obtención. Se suprimirán una vez transcurrido dicho plazo.

Artículo 11

Sanciones

Los Estados miembros establecerán las normas relativas a las sanciones aplicables a las infracciones del presente Reglamento y tomarán todas las medidas necesarias para garantizar su aplicación. Tales sanciones serán efectivas, proporcionadas y disuasorias.

A más tardar el 28 de diciembre de 2020, los Estados miembros notificarán a la Comisión las normas relativas a las sanciones aplicables a la introducción de bienes culturales en contravención del artículo 3, apartado 1, y las medidas relacionadas.

A más tardar el 28 de junio de 2025, los Estados miembros notificarán a la Comisión las normas relativas a las sanciones aplicables a otras infracciones al presente Reglamento, en particular la realización de declaraciones falsas y la presentación de información falsa, y las medidas relacionadas.

Los Estados miembros notificarán sin demora a la Comisión cualquier modificación posterior que afecte a dichas normas.

Artículo 12

Cooperación con terceros países

La Comisión podrá organizar, en materias que entren en su ámbito de actuación y en la medida necesaria para el desempeño de sus funciones en virtud del presente Reglamento, actividades de formación y capacitación para terceros países, en colaboración con los Estados miembros.

Artículo 13

Procedimiento de comité

1. La Comisión estará asistida por el comité creado en virtud del artículo 8 del Reglamento (CE) n.º 116/2009 del Consejo. 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, será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 14

Informes y evaluación

1. Los Estados miembros facilitarán a la Comisión información sobre la aplicación del presente Reglamento.

A tal fin, la Comisión enviará los cuestionarios pertinentes a los Estados miembros. Los Estados miembros tendrán seis meses, desde la recepción del cuestionario, para comunicar a la Comisión la información solicitada.

2. En el plazo de tres años a partir de la fecha en que el presente Reglamento sea aplicable en su totalidad, y posteriormente cada cinco años, la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre la aplicación del presente Reglamento. El informe se pondrá a disposición pública e incluirá la información estadística pertinente tanto en el ámbito de la Unión como a nivel nacional, como el número de licencias de importación expedidas, de solicitudes rechazadas y de declaraciones del importador presentadas. Incluirá un análisis de la aplicación práctica, incluidas las repercusiones para los operadores económicos de la Unión, en especial las pymes.

3. A más tardar el 28 de junio de 2020 y cada 12 meses hasta el establecimiento del sistema electrónico e contemplado en el artículo 9, la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre los avances realizados en la adopción de los actos de ejecución contemplados en el artículo 8, apartado 2, y en el establecimiento del sistema electrónico contemplado en el artículo 9.

Artículo 15

Entrada en vigor

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

Artículo 16

Aplicación

1. El presente Reglamento se aplicará a partir de la fecha de su entrada en vigor.

2. No obstante lo dispuesto en el apartado 1:

a) el artículo 3, apartado 1, se aplicará a partir del 28 de diciembre de 2020;

b) el artículo 3, apartados 2 a 5, 7 y 8, el artículo 4, apartados 1 a 10, el artículo 5, apartados 1 y 2, y el artículo 8, apartado 1, se aplicarán a partir de la fecha en que esté operativo el sistema electrónico a que se refiere el artículo 8 o a más tardar a partir del 28 de junio de 2025. La Comisión publicará en la serie C del *Diario Oficial de la Unión Europea* la fecha en la que se hayan cumplido las condiciones del presente apartado.

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

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

ANEXO

Parte A. Bienes culturales a los que se aplica el artículo 3, apartado 1

a)	Colecciones y ejemplares raros de zoología, botánica, mineralogía y anatomía, y objetos de interés paleontológico
b)	Bienes relacionados con la historia, con inclusión de la historia de las ciencias y de las técnicas, la historia militar y la historia social, así como con la vida de los dirigentes, pensadores, sabios y artistas nacionales y con los acontecimientos de importancia nacional
c)	Producto de las excavaciones (tanto autorizadas como clandestinas) o de descubrimientos arqueológicos, terrestres o subacuáticos
d)	Elementos procedentes de la desmembración de monumentos artísticos o históricos y de lugares de interés arqueológico ([1])
e)	Antigüedades que tengan más de 100 años, tales como inscripciones, monedas y sellos grabados
f)	Material etnológico
g)	Objetos de interés artístico tales como:
	i) cuadros, pinturas y dibujos hechos enteramente a mano sobre cualquier tipo de soporte y en cualquier material (con exclusión de los dibujos industriales y de los artículos manufacturados decorados a mano)
	ii) producciones originales de arte estatuario y de escultura en cualquier material
	iii) grabados, estampas y litografías originales
	iv) conjuntos y montajes artísticos originales en cualquier materia
h)	Manuscritos raros e incunables
i)	Libros, documentos y publicaciones antiguos de interés especial (histórico, artístico, científico, literario, etc.), sueltos o en colecciones
j)	Sellos de correo, sellos fiscales y análogos, sueltos o en colecciones
k)	Archivos, incluidos los fonográficos, fotográficos y cinematográficos
l)	Objetos de mobiliario que tengan más de 100 años e instrumentos de música antiguos

([1]) Se considerarán pertenecientes a esta categoría las estatuas e imágenes litúrgicas, incluso si son piezas aisladas.

Parte B. Bienes culturales a los que se aplica el artículo 4

Categorías de bienes culturales con arreglo a la parte A	Capítulo, partida o subpartida de la nomenclatura combinada (NC)	Umbral mínimo de antigüedad	Umbral mínimo financiero (valor en aduana)	Unidades suplementarias
c) Producto de las excavaciones (tanto autorizadas como clandestinas) o de descubrimientos arqueológicos, terrestres o subacuáticos	ex 9705; ex 9706	más de 250 años de antigüedad	cualquiera que sea el valor	número de artículos (p/st)
d) Elementos procedentes de la desmembración de monumentos artísticos o históricos y de lugares de interés arqueológico ([1])	ex 9705; ex 9706	más de 250 años de antigüedad	cualquiera que sea el valor	número de artículos (p/st)

([1]) Se considerarán pertenecientes a esta categoría las estatuas e imágenes litúrgicas, incluso si son piezas aisladas.

Parte C. Bienes culturales a los que se aplica el artículo 5

Categorías de bienes culturales con arreglo a la parte A	Capítulo, partida o subpartida de la nomenclatura combinada (NC)	Umbral mínimo de antigüedad	Umbral mínimo financiero (valor en aduana)	Unidades suplementarias
a) Colecciones y ejemplares raros de zoología, botánica, mineralogía y anatomía, y objetos de interés paleontológico	ex 9705	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
b) Bienes relacionados con la historia, con inclusión de la historia de las ciencias y de las técnicas, la historia militar y la historia social, así como con la vida de los dirigentes, pensadores, sabios y artistas nacionales y con los acontecimientos de importancia nacional	ex 9705	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
e) Antigüedades, tales como inscripciones, monedas y sellos grabados	ex 9706	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
f) Material etnológico	ex 9705	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
g) Objetos de interés artístico tales como:				
i) cuadros, pinturas y dibujos hechos enteramente a mano sobre cualquier tipo de soporte y en cualquier material (con exclusión de los dibujos industriales y de los artículos manufacturados decorados a mano)	ex 9701	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)

Categorías de bienes culturales con arreglo a la parte A	Capítulo, partida o subpartida de la nomenclatura combinada (NC)	Umbral mínimo de antigüedad	Umbral mínimo financiero (valor en aduana)	Unidades suplementarias
ii) producciones originales de arte estatuario y de escultura en cualquier material	ex 9703	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
iii) grabados, estampas y litografías originales	ex 9702	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
iv) conjuntos y montajes artísticos originales en cualquier materia	ex 9701	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
h) Manuscritos raros e incunables	ex 9702; ex 9706	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)
i) Libros, documentos y publicaciones antiguos de interés especial (histórico, artístico, científico, literario, etc.), sueltos o en colecciones	ex 9705; ex 9706	más de 200 años de antigüedad	18 000 EUR o más por artículo	número de artículos (p/st)

REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

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

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

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

Visto el dictamen del Comité de las Regiones ([2]),

De conformidad con el procedimiento legislativo ordinario ([3]),

Considerando lo siguiente:

(1) Las redes y los sistemas de información y las redes y servicios de comunicaciones electrónicas desempeñan un papel vital en la sociedad y se han convertido en la espina dorsal del crecimiento económico. Las tecnologías de la información y la comunicación (TIC) son la base de los complejos sistemas que sustentan las actividades cotidianas 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, organizaciones y empresas de toda la Unión está ya muy generalizada. La digitalización y la conectividad se están convirtiendo en elementos esenciales de un número cada vez mayor de productos y servicios, y con la llegada de la internet de las cosas, se espera que durante la próxima década se utilicen en la Unión un número extremadamente alto de dispositivos digitales conectados. 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, las organizaciones y las empresas de información suficiente sobre las características de ciberseguridad de los productos de ITC, servicios de TIC y los procesos de ITC, lo que socava la confianza en las soluciones digitales.

(3) La intensificación de la digitalización y de la conectividad trae consigo un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resulta más vulnerable a las ciberamenazas y se exacerban los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños. A fin de atenuar dichos riesgos, es preciso adoptar todas las medidas necesarias para mejorar la ciberseguridad en la Unión a fin de proteger mejor de las ciberamenazas a las redes y los sistemas de información, las redes de telecomunicaciones y los productos, los servicios y dispositivos digitales utilizados por los ciudadanos, las organizaciones y las empresas, desde las pequeñas y medianas empresas (pymes), según se definen en la Recomendación n.º 2003/361/CE ([4]) de la Comisión, a los operadores de infraestructuras críticas.

([1]) DO C 227 de 28.6.2018, p. 86.
([2]) DO C 176 de 23.5.2018, p. 29.
([3]) Posición del Parlamento Europeo de 12 de marzo de 2019 (pendiente de publicación el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.
([4]) Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

(4) Al hacer que la información pertinente esté a disposición del público, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) establecida por el Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo ([5]) contribuye al desarrollo del sector de la ciberseguridad en la Unión, en particular en lo que respecta a las pymes y las empresas emergentes. ENISA debe trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión y reforzar las cadenas de suministro de dentro de la Unión.

(5) Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y los ciberataques, requieren unas defensas más sólidas. Sin embargo, mientras que los ciberataques a menudo son transfronterizos, las competencias de las autoridades de ciberseguridad y policiales, así como las respuestas políticas de las mismas, son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la Unión. Esta situación requiere una respuesta efectiva y coordinada y una gestión de crisis a escala de la Unión, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad y la asistencia mutua en Europa. Además, es importante para los responsables políticos, la industria y los usuarios que se lleve a cabo una evaluación periódica del estado de la ciberseguridad y la resiliencia en la Unión, basada en datos fiables de la Unión, y que se haga una previsión sistemática de los avances, retos y amenazas futuros.

(6) A la luz de los crecientes retos a los que debe hacer frente 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. Dichos objetivos incluyen la necesidad de aumentar las capacidades y la preparación de los Estados miembros y de las empresas, así como de mejorar la cooperación, el intercambio de información y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la Unión. Por otra parte, habida cuenta de la naturaleza transfronteriza de las ciberamenazas, es necesario aumentar las capacidades de la Unión que podrían complementar la acción de los Estados miembros, en particular en el caso de ciberincidentes y crisis transfronterizas a gran escala, al tiempo que se ha de tener en cuenta la importancia de mantener y seguir mejorando las capacidades nacionales de respuesta a las ciberamenazas de cualquier envergadura.

(7) Son necesarios igualmente esfuerzos adicionales para aumentar la sensibilización de los ciudadanos, las organizaciones y las empresas sobre las cuestiones de ciberseguridad. Además, dado que los ciberincidentes merman la confianza en los proveedores de servicios digitales y en el propio mercado único digital, en especial entre los consumidores, debe reforzarse la confianza ofreciendo información transparente sobre el nivel de seguridad de los productos, servicios y procesos de TIC y subrayando que incluso un elevado nivel de certificación de la ciberseguridad no puede garantizar que un producto o servicio o proceso de TIC sea completamente seguro. Esto puede verse facilitado por una certificación a escala de la Unión que establezca requisitos y criterios de evaluación de la ciberseguridad comunes para todos los mercados y sectores nacionales.

(8) La ciberseguridad no es una cuestión meramente tecnológica sino que en ella desempeña un papel igualmente importante el comportamiento humano. Por ello, debe promoverse enérgicamente la «ciberhigiene», a saber, medidas sencillas de rutina que, aplicadas con regularidad por los ciudadanos, las organizaciones y las empresas, minimizan su exposición a los riesgos derivados de las ciberamenazas.

(9) Con el fin de reforzar las estructuras de ciberseguridad de la Unión, es importante mantener y desarrollar las capacidades de los Estados miembros para responder globalmente a las ciberamenazas, incluidos los incidentes transfronterizos.

(10) Las empresas y los consumidores particulares deben disponer de información precisa sobre el nivel de garantía con el que se ha certificado la seguridad de sus productos, servicios y procesos de TIC. Al mismo tiempo, ningún producto o servicio de TIC es totalmente ciberseguro y se deben promover y priorizar normas básicas de ciberhigiene. Habida cuenta de la creciente disponibilidad de dispositivos de la internet de las cosas, hay una serie de medidas voluntarias que el sector privado puede adoptar para reforzar la confianza en la seguridad de los productos, servicios y procesos de TIC.

(11) A menudo, los modernos productos y sistemas de TIC integran una o varias tecnologías y componentes de terceros y se basan en ellos, por ejemplo, módulos de programas, bibliotecas o interfaces de programación de aplicaciones. Esta relación, llamada de «dependencia», puede presentar riesgos adicionales en materia de ciberseguridad, pues las vulnerabilidades de los componentes de terceros pueden afectar también a los productos, servicios y procesos de TIC. En gran número de casos, determinar y documentar dichas dependencias permite a los usuarios finales de los productos, servicios y procesos de TCI optimizar sus actividades de gestión relacionadas con la ciberseguridad mejorando, por ejemplo, los procedimientos que ponen a punto para detectar las vulnerabilidades en materia de ciberseguridad y ponerles remedio.

([5]) 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).

(12) Las organizaciones, fabricantes y proveedores implicados en el diseño y desarrollo de productos, servicios y procesos de TIC deben ser animadas a aplicar medidas desde las primeras fases del diseño y desarrollo que permitan proteger desde el principio y en la máxima medida posible la seguridad de tales productos, procesos y servicios, presuponer que se van a producir ataques y prever y limitar sus repercusiones («seguridad desde el diseño»). La seguridad se debe tener en cuenta durante todo el ciclo de vida del producto, servicio o proceso de TIC y los procesos de diseño y desarrollo deben evolucionar constantemente para reducir el riesgo de daños derivados de la explotación malintencionada.

(13) Las empresas, las organizaciones y el sector público que participan en el diseño deben configurar los productos, servicios o procesos de TIC de manera que se garantice un nivel de seguridad más elevado, lo que debe permitir que el primer usuario reciba una configuración por defecto que sea lo más segura posible (en lo sucesivo, «seguridad por defecto»), de modo que se reduzca la carga del usuario de configurar el producto, servicio o proceso de TIC de manera adecuada. La seguridad por defecto debe funcionar sin que sea necesaria una configuración minuciosa, unos conocimientos técnicos específicos o un comportamiento no evidente por parte del usuario y debe funcionar fácilmente y de manera fiable cuando se aplique. Si del análisis de riesgos y de manejabilidad, que se llevará a cabo caso por caso, se desprende que tal configuración no es viable, se deberá incitar a los usuarios a optar por la configuración más segura.

(14) El Reglamento (CE) n.º 460/2004 del Parlamento Europeo y del Consejo ([6]) creó ENISA con el objetivo de contribuir al establecimiento de un elevado y efectivo nivel de seguridad de las redes y de la información en la Unión y al desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las administraciones públicas. El Reglamento (CE) n.º 1007/2008 del Parlamento Europeo y del Consejo ([7]), prorrogó el mandato de ENISA hasta marzo de 2012. El Reglamento (UE) n.º 580/2011 del Parlamento Europeo y del Consejo ([8]) prorrogó nuevamente el mandato de ENISA hasta el 13 de septiembre de 2013. El Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo ha prorrogado el mandato de ENISA hasta el 19 de junio de 2020.

(15) 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 Unión Europea 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 ciudadanos en línea, el primer acto jurídico en el ámbito de la ciberseguridad de la Unión fue adoptado en 2016, fue la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([9]). La Directiva (UE) 2016/1148 instauró una serie de 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 de la economía y la sociedad, como la energía, los transportes, el agua potable, el suministro y la distribución, la banca, las infraestructuras de los mercados financieros, la sanidad o las infraestructuras digitales, así como para los proveedores de servicios digitales clave (motores de búsqueda, servicios en la nube y mercados en línea).

Se atribuyó un papel clave a ENISA para respaldar la aplicación de dicha Directiva. Además, la lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, que contribuye al objetivo general de conseguir un elevado nivel de ciberseguridad. También contribuyen al elevado nivel de ciberseguridad en el mercado único digital otros actos jurídicos, como el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([10]) y las Directivas 2002/58/CE ([11]) y (UE) 2018/1972 ([12]) del Parlamento Europeo y del Consejo.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

([10]) 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).

([11]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([12]) Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

(16) Desde la adopción de la Estrategia de Ciberseguridad de la Unión Europea en 2013 y la última revisión del mandato de ENISA, el contexto político general ha cambiado considerablemente y el contexto mundial ha pasado a ser más incierto y menos seguro. En este contexto y en el marco de la positiva evolución del cometido de ENISA a lo largo de los años como punto de referencia en materia de asesoramiento y conocimientos y como facilitadora de la coordinación y el desarrollo de capacidades, así como 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 nuevo ecosistema de la ciberseguridad y garantizar que contribuya eficazmente a configurar la respuesta de la Unión a los desafíos de ciberseguridad derivados de la transformación radical de las amenazas, para lo cual, como reconoció la evaluación de ENISA, el mandato actual resulta insuficiente.

(17) ENISA tal como se establece en el presente Reglamento debe suceder a ENISA tal como fue creada por el Reglamento (UE) n.º 526/2013. ENISA debe llevar a cabo las tareas que le confiere el presente Reglamento y otros 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 y los Estados miembros, actuando como punto de referencia para las iniciativas políticas sectoriales de la Unión en lo que respecta a la ciberseguridad y fomentando la cooperación operativa tanto entre los Estados miembros, como entre los Estados miembros y las instituciones, órganos y organismos de la Unión.

(18) En el marco de la Decisión 2004/97/CE, Euratom, tomada de común acuerdo por los representantes de los Estados miembros, reunidos a nivel de jefes de Estado o de Gobierno ([13]), 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 ENISA debe ofrecer las mejores condiciones posibles para su funcionamiento correcto y eficaz. Para el desempeño correcto y eficaz de sus funciones, para atraer y conservar al personal y para establecer contactos con el exterior de manera más eficaz, es imperativo que ENISA 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 ENISA y el Estado miembro anfitrión, cuya celebración ha de contar con la aprobación del Consejo de Administración de ENISA.

(19) En vista de los crecientes riesgos y amenazas en materia de ciberseguridad a los que debe hacer frente la Unión, deben incrementarse los recursos financieros y humanos asignados a ENISA, en consonancia con la ampliación de sus cometidos y tareas, así como su posición crucial en el ecosistema de organizaciones que defienden el ecosistema digital de la Unión, a fin de permitir que ENISA pueda desempeñar eficazmente las tareas que le encomienda el presente Reglamento.

(20) ENISA 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, la transparencia de sus métodos de funcionamiento y su diligencia en el desempeño de sus tareas. ENISA debe apoyar activamente los esfuerzos nacionales y contribuir proactivamente a los esfuerzos de la Unión y desempeñar sus funciones cooperando plenamente con las instituciones, órganos y organismos de la Unión y con los Estados miembros, evitando la duplicación de tareas y promoviendo las sinergias. Además, ENISA debe apoyarse en las aportaciones del sector privado y otras partes interesadas pertinentes y en la cooperación con tales agentes.

La manera en que ENISA debe alcanzar sus objetivos se debe definir a través de un conjunto de tareas que permita cierta flexibilidad en su funcionamiento.

(21) Para poder prestar un apoyo adecuado a la cooperación operativa entre los Estados miembros, ENISA debe seguir reforzando sus capacidades y destrezas técnicas y humanas. ENISA debe reforzar sus conocimientos técnicos y capacidades. ENISA y los Estados miembros pueden, de forma voluntaria, elaborar programas para la comisión de servicios de expertos nacionales en ENISA, la creación de contingentes de expertos y el intercambio de personal.

(22) ENISA debe prestar asistencia a la Comisión mediante asesoramiento, dictámenes y análisis en todos los asuntos de la Unión relacionados con la formulación, la actualización y la revisión de políticas y disposiciones legislativas en el ámbito de la ciberseguridad y sus aspectos sectoriales para potenciar la pertinencia de las políticas y la legislación de la Unión que presenten aspectos relacionados con la ciberseguridad y permitir la coherencia en su aplicación a nivel nacional. La Agencia debe actuar como punto de referencia de asesoramiento y conocimientos en relación con las iniciativas políticas y legislativas sectoriales de la Unión, cuando intervengan cuestiones relacionadas con la ciberseguridad. ENISA debe informar periódicamente al Parlamento Europeo de sus actividades.

([13]) Decisión 2004/97/CE, Euratom adoptada de común acuerdo por los Representantes de los Estados miembros, reunidos a escala de Jefes de Estado o de Gobierno, de 13 de diciembre de 2003, relativa a la fijación de las sedes de determinadas oficinas y agencias de la Unión Europea (DO L 29 de 3.2.2004, p. 15).

(23) El núcleo público de la internet abierta, consistente en sus protocolos e infraestructura principales, que constituyen un bien público mundial, posibilita la funcionalidad esencial de internet en su conjunto, y en él se sustenta su funcionamiento normal. ENISA debe promover la seguridad una internet pública esencial y abierta y la estabilidad de su funcionamiento, lo que incluye, a título meramente enunciativo, sus protocolos esenciales (en particular, DNS, BGP e IPv6), el funcionamiento del sistema de nombres de dominio (incluido el funcionamiento de todos los dominios de nivel superior) y el funcionamiento de la zona raíz.

(24) La principal tarea de ENISA es promover la aplicación coherente del marco jurídico pertinente, en particular la aplicación efectiva de la Directiva (UE) 2016/1148 y otros instrumentos jurídicos pertinentes que contienen disposiciones en materia de ciberseguridad, lo 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.

(25) ENISA debe asistir a los Estados miembros y a las instituciones, órganos y organismos de la Unión en sus esfuerzos por crear y mejorar su capacidad y preparación para prevenir, detectar y dar respuesta a las ciberamenazas y los ciberincidentes, así como en relación con la seguridad de las redes y los sistemas de información. En particular, ENISA debe prestar apoyo al establecimiento y mejora de los equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «CSIRT», por sus siglas en inglés de «computer security incident response teams») nacionales y de la Unión previstos en la Directiva (UE) 2016/1148 con vistas a alcanzar un elevado nivel común de madurez en la Unión. Las actividades realizadas por ENISA en relación con las capacidades operativas de los Estados miembros deben respaldar activamente las acciones emprendidas por los Estados miembros para el cumplimiento de sus obligaciones en virtud de la Directiva (UE) 2016/1148 y no deben, por tanto, sustituirlas.

(26) ENISA también debe prestar asistencia en la elaboración y actualización de las estrategias en materia de seguridad de las redes y los sistemas de información a escala de la Unión y, previa solicitud, a escala de los Estados miembros, en particular, en materia de ciberseguridad, y debe promover la difusión de dichas estrategias y hacer un seguimiento de los avances en su aplicación. Asimismo, ENISA debe ofrecer aportaciones para satisfacer la necesidad de cursos y material de formación, en particular a los organismos públicos y, cuando proceda, y en gran medida, «formar formadores», sobre la base del Marco de Competencias Digitales para los Ciudadanos con el fin de ayudar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a desarrollar sus propias capacidades de formación.

(27) ENISA debe apoyar a los Estados miembros en el ámbito de la sensibilización y la educación en materia de ciberseguridad facilitando una coordinación más estrecha y el intercambio de mejores prácticas entre los Estados miembros. Dicho apoyo debe consistir en la creación de una red de puntos de contacto nacionales en materia de educación y en el establecimiento de una plataforma de formación sobre ciberseguridad. La red de puntos de contacto nacionales en materia de educación puede funcionar en el marco de la red de funcionarios de enlace nacionales y servir de punto de partida para la coordinación futura dentro de los Estados miembros.

(28) ENISA debe asistir al Grupo de cooperación creado por la Directiva (UE) 2016/1148 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, así como en relación con las dependencias transfronterizas, en lo que se refiere a riesgos e incidentes.

(29) Con el fin de estimular la cooperación entre los sectores público y privado y dentro del sector privado, en particular para apoyar la protección de las infraestructuras críticas, ENISA debe animar a que los sectores intercambien información entre sí y también en su propio seno, en particular aquellos que figuran en el anexo II de la Directiva (UE) 2016/1148, 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, por ejemplo, facilitando la creación de centros sectoriales de puesta en común y análisis de la información).

(30) Mientras el posible impacto negativo de las vulnerabilidades detectadas en los productos, servicios y procesos de TIC siga aumentando, será de vital importancia identificarlas y subsanarlas con el fin de reducir los riesgos generales en materia de ciberseguridad. Se ha demostrado que la cooperación entre organizaciones, fabricantes o proveedores de productos, servicios y procesos de TIC vulnerables y los miembros de la comunidad investigadora en materia de ciberseguridad y las autoridades encargadas de la identificación de dichas vulnerabilidades aumenta considerablemente la tasa de identificación y corrección de las vulnerabilidades detectadas en los productos, servicios y procesos de TIC. La divulgación coordinada de vulnerabilidades es un proceso estructurado de cooperación en el que se informa al propietario del sistema de información de las vulnerabilidades detectadas, lo que ofrece a la organización la oportunidad de identificar y subsanar una vulnerabilidad antes de que la información detallada relacionada con esta se haga pública o pueda divulgarse a terceros. Este proceso facilita además la coordinación entre el identificador y la organización en lo que respecta a la publicación de dichas vulnerabilidades. Las políticas de la divulgación coordinada de vulnerabilidades pueden desempeñar un papel importante en los esfuerzos de los Estados miembros por mejorar la ciberseguridad.

(31) ENISA debe agregar y analizar, compartidos de forma voluntaria, los informes nacionales de los CSIRT y del equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) establecido por el Acuerdo entre el Parlamento Europeo, el Consejo Europeo, el Consejo de la Unión Europea, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo, el Tribunal de Cuentas Europeo, el Servicio Europeo de Acción Exterior, el Comité Económico y Social Europeo, el Comité Europeo de las Regiones y el Banco Europeo de Inversiones sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) ([14]), a los efectos de contribuir al establecimiento de unos procedimientos, un lenguaje y una terminología comunes para el intercambio de información. En este contexto, ENISA debe fomentar la participación del sector privado, en el marco de la Directiva (UE) 2016/1148, que establece las bases para el intercambio voluntario de información técnica a nivel operativo dentro de la red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red CSIRT») creada por dicha Directiva.

(32) ENISA debe contribuir a aportar una respuesta a nivel de la Unión en caso de incidentes y crisis transfronterizos a gran escala relacionados con la ciberseguridad. Esta tarea debe desempeñarse conforme al mandato de ENISA en virtud del presente Reglamento y a una fórmula que acordarán los Estados miembros en el contexto de la Recomendación (UE) 2017/1584 ([15]) de la Comisión y a las conclusiones del Consejo de 26 de junio de 2018 sobre la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala. La citada tarea podría incluir la recogida de información pertinente y el desempeño del papel de mediador entre la red de CSIRT y la comunidad técnica, así como entre los responsables políticos de gestionar la crisis. Por otra parte, ENISA debe apoyar la cooperación operativa entre Estados miembros, a petición de uno o más Estados miembros, para el tratamiento de incidentes desde una perspectiva técnica facilitando el intercambio de soluciones técnicas pertinentes entre los Estados miembros y aportando información a las comunicaciones públicas. ENISA debe apoyar la cooperación operativa ensayando las disposiciones de esa cooperación a través de ejercicios periódicos de ciberseguridad.

(33) Al apoyar la cooperación operativa, ENISA debe hacer uso de las competencias técnicas y operativas disponibles del CERT-UE a través de una cooperación estructurada. La cooperación estructurada puede permitir acumular conocimientos a ENISA. Cuando proceda, deben establecerse disposiciones específicas adecuadas entre las dos entidades para definir los aspectos prácticos de dicha cooperación y evitar la duplicación de actividades.

(34) Al desempeñar sus tareas de apoyo de la cooperación operativa dentro de la red de CSIRT, ENISA debe poder prestar ayuda a los Estados miembros si estos se la piden, por ejemplo, asesorándolos sobre el modo de mejorar sus capacidades para prevenir, detectar y responder ante incidentes, facilitando la gestión técnica de incidentes que tengan un impacto significativo o sustancial o garantizando que se realicen análisis de ciberamenazas e incidentes. ENISA debe facilitar la gestión técnica de los incidentes que tengan un impacto significativo o sustancial, en particular, apoyando el intercambio voluntario de soluciones técnicas entre Estados miembros o aporte información técnica combinada, como las soluciones técnicas que pongan en común voluntariamente los Estados miembros. La Recomendación (UE) 2017/1584 recomienda que los Estados miembros cooperen de buena fe y compartan entre ellos y con ENISA información sobre las crisis e incidentes a gran escala relacionados con la ciberseguridad sin demora indebida. Dicha información debe servir de ayuda a ENISA en el desempeño de sus funciones de apoyo a la cooperación operativa.

(35) Dentro de la cooperación regular a nivel técnico para ayudar a la Unión a conocer la situación, ENISA, en estrecha cooperación con los Estados miembros, debe elaborar periódicamente un informe detallado de situación técnica en materia de ciberseguridad de la UE sobre incidentes y ciberamenazas, basándose en la información públicamente disponible, en su propio análisis y en los informes compartidos por los CSIRT de los Estados miembros o los puntos de contacto únicos nacionales sobre la seguridad de las redes y sistemas de información (en lo sucesivo, «puntos de contacto únicos») previstos en la Directiva (UE) 2016/1148 (ambos de forma voluntaria), el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y, cuando proceda, el Centro de Análisis de Inteligencia de la Unión Europea (UE-INTCEN) del Servicio Europeo de Acción Exterior (. Dicho informe debe ponerse a disposición del Consejo, la Comisión, la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y la red de CSIRT.

(36) El apoyo de ENISA a las investigaciones técnicas *ex post* en relación con incidentes con efectos significativos facilitado a petición de los Estados miembros afectados debe centrarse en la prevención de incidentes futuros. Los Estados miembros afectados deben proporcionar la información y asistencia necesarias para que ENISA pueda apoyar de forma efectiva la investigación técnica *ex post*.

([14]) DO C 12 de 13.1.2018, p. 1.

([15]) Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

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

(38) 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 a las instituciones, órganos y organismos de la Unión, ENISA necesita analizar los riesgos actuales y emergentes de ciberseguridad. A tal efecto, ENISA, en cooperación con los Estados miembros y, si procede, con los organismos estadísticos o de otro tipo, debe recopilar la información pertinente que esté disponible públicamente o se comparta de forma voluntaria 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, ENISA debe apoyar a los Estados miembros y a las instituciones, órganos y organismos de la Unión a la hora de detectar nuevos riesgos relacionados con la ciberseguridad y prevenir los incidentes, mediante la realización de análisis de ciberamenazas, vulnerabilidades e incidentes.

(39) Con el fin de aumentar la resiliencia de la Unión, ENISA debe impulsar conocimientos en el ámbito de la ciberseguridad de las infraestructuras prestando apoyo, en particular, a los sectores recogidos en el anexo II de la Directiva (UE) 2016/1148 y los que utilicen los proveedores de servicios digitales que figuran en el anexo III de dicha Directiva, ofreciendo asesoramiento y orientaciones e intercambiando mejores prácticas. Con el fin de facilitar el acceso a una información mejor estructurada sobre los riesgos relacionados con la ciberseguridad y las posibles soluciones, ENISA 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 Unión. Facilitar el acceso a una información mejor estructurada sobre los riesgos relacionados con la ciberseguridad y las posibles soluciones también puede ayudar a los Estados miembros a consolidar sus capacidades, a alinear sus prácticas y, por ende, a mejorar su resiliencia general frente a los ciberataques.

(40) ENISA debe contribuir a la sensibilización del público sobre los riesgos relacionados con la ciberseguridad, en particular mediante una campaña de sensibilización a nivel europeo y la promoción de la educación, y facilitar orientaciones sobre buenas prácticas para usuarios individuales dirigidas a ciudadanos, organizaciones y empresas. ENISA debe contribuir asimismo a promover las mejores prácticas y soluciones, incluidas la ciberhigiene y la ciberalfabetización de los ciudadanos, a nivel de ciudadanos, organizaciones y empresas mediante la recogida y el análisis de la información disponible públicamente relativa a incidentes significativos, y mediante la elaboración y publicación de informes y orientaciones para ciudadanos, organizaciones y empresas y mejorar el nivel general de preparación y resiliencia. ENISA también debe trabajar para proporcionar a los consumidores la correspondiente información acerca de los esquemas de certificación aplicables, por ejemplo, ofreciendo orientaciones y recomendaciones. ENISA debe además organizar, en consonancia con el Plan de Acción de Educación Digital establecido en la Comunicación de la Comisión de 17 de enero de 2018 y en colaboración con los Estados miembros y las instituciones, agencias y organismos de la Unión, campañas sistemáticas de comunicación y educación pública destinadas a los usuarios finales, con miras a promover comportamientos individuales en línea más seguros y la alfabetización digital y a concienciar sobre las ciberamenazas potenciales, incluyendo actividades criminales en línea como los ataques por suplantación de identidad (phishing), las redes infectadas (botnets) o los fraudes bancarios y financieros, e incidentes de fraude en materia de datos, así como dar consejos básicos en materia de autenticaciones multifactores, correcciones, cifrado, anonimización y protección de datos.

(41) ENISA debe desempeñar un papel central para acelerar la sensibilización de los usuarios finales con respecto a la seguridad de los dispositivos y el uso seguro de los servicios, promoviendo a nivel de la Unión la seguridad y la protección de la intimidad desde la concepción de los mismos. Para lograr ese objetivo, ENISA debe aprovechar al máximo las mejores prácticas y experiencias existentes, en especial las de las instituciones académicas y de los investigadores en materia de seguridad informática.

(42) 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, ENISA 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.

(43) ENISA debe contribuir a los esfuerzos de la Unión de cooperar con organismos internacionales y en marcos de cooperación internacional pertinentes en el ámbito de la ciberseguridad. En particular, ENISA debe contribuir, cuando proceda, a la cooperación con organismos tales como la OCDE, la OSCE y la OTAN. Dicha cooperación podría incluir la realización de ejercicios conjuntos de ciberseguridad y la coordinación conjunta de la respuesta a incidentes. Dichas actividades deben realizarse respetando plenamente los principios de inclusión, reciprocidad y autonomía del proceso decisorio de la Unión, sin perjuicio del carácter específico de la política de seguridad y defensa de los Estados miembros.

(44) Para asegurar que cumple plenamente sus objetivos, ENISA debe permanecer en contacto con las correspondientes autoridades de supervisión de la Unión y otras autoridades competentes de la Unión, instituciones, órganos y organismos de la Unión, incluidos el CERT-UE, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, Agencia Europea de Defensa (AED), la Agencia del Sistema Global de Navegación por Satélite Europeo (Agencia del GNSS Europeo), el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), la Agencia Europea para la Gestión Operativa de los Sistemas Informáticos de Gran Magnitud en el espacio de libertas, seguridad y justicia (eu-LISA), el Banco Central Europeo (BCE), la Autoridad Bancaria Europea (ABE), el Comité Europeo de Protección de Datos, la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (ACER), la Agencia Europea de Seguridad Aérea (EASA) y cualquier otro órgano de la Unión relacionado con la ciberseguridad.

ENISA 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 Consultivo de ENISA. En sus relaciones con las autoridades encargadas de hacer cumplir la ley sobre aspectos relacionados con la seguridad de las redes y de la información que puedan tener repercusiones en su trabajo, ENISA debe respetar los canales de información y las redes existentes.

(45) Pueden establecerse asociaciones con instituciones académicas que desarrollen iniciativas de investigación en los ámbitos pertinentes, y deben contar con cauces apropiados de las aportaciones de las organizaciones de consumidores y otras organizaciones, que deben tenerse en cuenta.

(46) ENISA, en su función de secretaría de la red de CSIRT, 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 (UE) 2016/1148. Además, ENISA 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 CSIRT, teniendo siempre debidamente en cuenta los procedimientos operativos estándar de la red de CSIRT.

(47) Con el fin de aumentar la preparación de la Unión para una respuesta a los incidentes, ENISA debe organizar periódicamente 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 Unión en la organización de ejercicios. Los ejercicios exhaustivos de seguridad a gran escala en el que se incluyan elementos técnicos, operativos y estratégicos deben organizarse cada dos años. Además, ENISA debe poder organizar periódicamente ejercicios menos exhaustivos con el mismo objetivo de mejorar la preparación de la Unión para responder a los incidentes.

(48) ENISA 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. ENISA debe aprovechar las buenas prácticas existentes y 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 (marco europeo de certificación de la ciberseguridad), con el fin de aumentar la transparencia de la garantía de la ciberseguridad de los productos, servicios y procesos de TIC y reforzar así la confianza en el mercado interior digital, así como su competitividad.

(49) Unas políticas de ciberseguridad eficientes deben basarse en métodos de evaluación de riesgos bien elaborados, 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, ENISA debe apoyar la cooperación entre las partes interesadas a escala de la Unión y facilitar 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.

(50) ENISA debe alentar a los Estados miembros, a los fabricantes o los proveedores de productos, servicios o procesos de TIC 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 y deben dar incentivos para ello. En particular, los fabricantes y proveedores de productos, servicios o procesos de TIC deben aportar las actualizaciones necesarias y recuperar, retirar o reciclar los productos, servicios o procesos de TIC que no cumplan las normas de ciberseguridad, mientras que los importadores y distribuidores deben asegurarse de que los productos, servicios y procesos de TIC que introduzcan en el mercado de la Unión cumplen los requisitos aplicables y no supongan un riesgo para los consumidores de la Unión.

(51) En cooperación con las autoridades competentes, ENISA debe poder difundir información relativa al nivel de ciberseguridad de los productos, servicios y procesos de TIC ofrecidos en el mercado interior, y emitir advertencias dirigidas a los fabricantes y los proveedores de productos, servicios o procesos de TIC solicitándoles que mejoren la seguridad de los mismos, incluida la ciberseguridad.

(52) ENISA 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 ciberseguridad. A fin de determinar las necesidades y prioridades en materia de investigación, ENISA debe consultar asimismo a los grupos de usuarios pertinentes. Más concretamente, puede establecerse una cooperación con el Consejo Europeo de Investigación y el Instituto Europeo de Innovación y Tecnología, así como con el Instituto de Estudios de Seguridad de la Unión Europea.

(53) ENISA debe consultar de forma regular a organizaciones de normalización, en particular a organizaciones de normalización europeas, a la hora de preparar los esquemas europeos de certificación de la ciberseguridad.

(54) Las ciberamenazas tienen un alcance mundial. Es necesaria una cooperación internacional más estrecha para mejorar las normas de ciberseguridad, incluida la necesidad de definir normas de comportamiento comunes, la adopción de códigos de conducta, el uso de normas internacionales 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, y promueva un enfoque mundial común al respecto. A tal efecto, ENISA 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 correspondientes instituciones, órganos y organismos de la Unión.

(55) ENISA 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 Unión en materias que correspondan al mandato de ENISA.

(56) Es razonable y recomendable aplicar determinados principios relativos a la gobernanza de ENISA para cumplir con la declaración conjunta y el enfoque común aprobados en julio de 2012 por el Grupo de trabajo interinstitucional sobre las agencias descentralizadas, cuya finalidad es la racionalización las actividades de las agencias descentralizadas y la mejora de su funcionamiento. Las recomendaciones de la declaración conjunta y el enfoque común también han de quedar reflejados, cuando proceda, en los programas de trabajo de ENISA, sus evaluaciones y sus prácticas administrativas y de presentación de informes.

(57) El Consejo de Administración, integrado por los representantes de Estados miembros y de la Comisión, debe establecer la orientación general del funcionamiento de ENISA 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 ENISA, adoptar el documento único de programación de ENISA, adoptar su propio reglamento interno, nombrar al director ejecutivo y decidir la prórroga y terminación del mandato del director ejecutivo.

(58) Para que ENISA 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 y de experiencia adecuadas. 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.

(59) Para un buen funcionamiento de ENISA, 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 anual de ENISA, 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 incluya la aplicación del programa de trabajo anual de ENISA que presentará al Consejo de Administración, redactar un proyecto de declaración de las previsiones de ingresos y gastos de ENISA y ejecutar el presupuesto. Además, el director ejecutivo debe tener la posibilidad de crear grupos de trabajo *ad hoc* para que examinen asuntos concretos, en particular los de índole científica, técnica, jurídica o socioeconómica. En particular, en relación con la preparación de una propuesta de esquema específica de certificación europea de ciberseguridad (en lo sucesivo, «propuesta de esquema»), la creación de un grupo de trabajo *ad hoc* se considera necesaria. 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 y de género, según proceda en función de las cuestiones específicas de que se trate, entre las administraciones públicas de los Estados miembros, las instituciones, órganos y organismos de la Unión, el sector privado, incluida la industria, los usuarios y los expertos académicos en seguridad de las redes y de la información.

(60) 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, el Comité Ejecutivo debe examinar en detalle la información pertinente, explorar las opciones disponibles y ofrecer asesoramiento y soluciones para preparar las decisiones del Consejo de Administración.

(61) ENISA debe contar con un Grupo Consultivo de ENISA 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 Consultivo de ENISA, 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 ENISA. El Grupo Consultivo de ENISA debe ser consultado en particular en lo que se refiere al proyecto de programa de trabajo anual. La composición del Grupo Consultivo de ENISA y las tareas asignadas a este grupo deben garantizar una representación suficiente de las partes interesadas en los trabajos de ENISA.

(62) Debe crearse el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad para ayudar a ENISA y a la Comisión a facilitar la consulta de las partes interesadas pertinentes. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad debe estar compuesto por miembros que representen a la industria en una proporción equilibrada, tanto del lado de la demanda como de la oferta de productos y servicios de TIC, y entre ellos, en particular, las pymes, los proveedores de servicios digitales, los organismos de normalización europeos e internacionales, los organismos nacionales de acreditación, las autoridades de supervisión de la protección de datos y los organismos de evaluación de la conformidad en virtud del Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([16]), el mundo académico y las organizaciones de consumidores.

(63) ENISA debe instaurar normas para la prevención y gestión de los conflictos de intereses. ENISA 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 ([17]). Los datos personales deben ser tratados por ENISA de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([18]),. ENISA debe cumplir las disposiciones aplicables a las instituciones, órganos y organismos 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 Unión Europea (ICUE).

(64) Con el fin de garantizar la plena autonomía e independencia de ENISA 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 ENISA. Es primordial que ENISA disponga de un presupuesto adecuado de modo que disponga de la capacidad suficiente para cumplir todos sus cometidos y objetivos, que cada vez son mayores. La mayor parte del personal de ENISA debe estar dedicado directamente a la ejecución operativa del mandato de ENISA. Debe permitirse que el Estado miembro anfitrión, o cualquier otro Estado miembro, efectúe aportaciones voluntarias a los ingresos de ENISA. 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 ENISA para garantizar la transparencia y la responsabilidad.

(65) La certificación de la ciberseguridad desempeña un importante papel a la hora de aumentar la confianza y la seguridad en los productos, servicios y procesos 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, servicios y procesos ofrecen un determinado nivel 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 (UE) 2016/1148 resulta crítica la certificación de la ciberseguridad.

([16]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 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 (DO L 218 de 13.8.2008, p. 30).

([17]) 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).

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

(66) 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, servicios y procesos 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 Unión es otra de las carencias que padece el mercado único de la ciberseguridad. Esto hace difícil que las empresas europeas compitan a nivel nacional, de la Unión y mundial. Ello también 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 comunicación de 2017 sobre la aplicación de la Estrategia para el Mercado Único Digital-Un Mercado Único Digital conectado para todos, 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 interior.

(67) En la actualidad, la certificación de la ciberseguridad de los productos, servicios y procesos de TIC se utiliza solo en medida limitada. Cuando existe, es principalmente a nivel de los Estados miembros o en el marco de esquemas impulsados por la industria. En este contexto, un certificado expedido por una autoridad nacional de certificación de la ciberseguridad no se ve reconocido en principio por los demás Estados miembros. Así, las empresas pueden tener que certificar sus productos, servicios y procesos TIC en los distintos Estados miembros en que operen, con vistas, por ejemplo, a tomar parte en procedimientos de contratación nacionales, con el correspondiente aumento de sus costes. Por otra parte, aun cuando están surgiendo nuevos esquemas, 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 esquemas existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real, lo que crea dificultades a los mecanismos de reconocimiento mutuo dentro de la Unión.

(68) Se han realizado esfuerzos en el pasado para velar por el reconocimiento mutuo de los certificados dentro de la Unión, 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 SOG-IS incluye solo a algunos Estados miembros. Esto ha limitado la eficacia del ARM del SOG-IS desde el punto de vista del mercado interior.

(69) Por consiguiente, es necesario adoptar un planteamiento común y establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar esquemas europeos de certificación de la ciberseguridad y permita que los certificados de ciberseguridad europeos y las declaraciones de conformidad de la UE de productos, servicios o procesos de TIC sean reconocidos y usados en todos los Estados miembros. A este respecto, es esencial basarse en los esquemas nacionales e internacionales existentes, así como en los sistemas de reconocimiento mutuo, en particular el SOG-IS, y permitir una transición fluida de los esquemas existentes bajo dichos sistemas a los esquemas del nuevo marco europeo de certificación de la ciberseguridad. El marco europeo de certificación de la ciberseguridad. debe tener un doble objetivo. Primero, debe contribuir a aumentar la confianza en los productos, servicios y procesos de TIC que hayan sido certificados con arreglo a los esquemas europeos de certificación de la ciberseguridad. Segundo, evitar la multiplicación de los esquemas 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 esquemas europeos de certificación de la ciberseguridad deben ser no discriminatorios y basarse en normas internacionales o europeas, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la Unión al respecto.

(70) El marco europeo de certificación de la ciberseguridad debe implantarse de forma uniforme en todos los Estados miembros, a fin de evitar la práctica de escoger entre ellos en función de las diferencias en los niveles de exigencia en diferentes Estados miembros.

(71) Los esquemas europeos de certificación de la ciberseguridad deben basarse en los ya existentes a nivel nacional e internacional y, de ser necesario, en especificaciones técnicas de foros y consorcios, aprendiendo de los puntos fuertes actuales y evaluando y corrigiendo los puntos débiles.

(72) Se necesitan soluciones de ciberseguridad flexibles para que la industria vaya por delante de las ciberamenazas y, por tanto, cualquier esquema de certificación debe concebirse de tal manera que se evite el riesgo de quedarse rápidamente desfasado.

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

(74) Las disposiciones del presente Reglamento deben entenderse sin perjuicio de la legislación de la Unión que fija normas específicas sobre la certificación de productos, servicios y procesos de TIC. En particular, el Reglamento (UE) 2016/679 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, servicios y procesos de TIC. El presente Reglamento se entiende sin perjuicio de la certificación de las operaciones de tratamiento de datos en el marco del Reglamento (UE) 2016/679, incluso cuando dichas operaciones se encuentran integradas en productos, servicios y procesos de TIC.

(75) El objetivo de los esquemas europeos de certificación de la ciberseguridad debe ser garantizar que los productos, servicios y procesos de TIC certificados con arreglo a un esquema cumplan los requisitos especificados con objeto de proteger la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, servicios y procesos a lo largo de su ciclo de vida, o los servicios ofrecidos por ellos o accesibles a través de ellos. No es posible definir con detalle los requisitos de ciberseguridad relativos a todos los productos, servicios y procesos de TIC en el presente Reglamento. Los productos, servicios y procesos de TIC y las necesidades de ciberseguridad relativas a dichos productos, servicios y procesos son tan dispares que es muy difícil elaborar unos requisitos de ciberseguridad generales que sean válidos en todas las circunstancias. Por lo tanto, es necesario adoptar un concepto amplio y general de la ciberseguridad a efectos de la certificación, que debe ser complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los esquemas europeos de certificación de ciberseguridad. Las disposiciones con que se lograrán tales objetivos para determinados productos, servicios y procesos de TIC deben especificarse luego con más detalle a nivel de cada esquema de certificación adoptado por la Comisión, por ejemplo, mediante referencia a normas o especificaciones técnicas cuando no se disponga de normas apropiadas.

(76) Las especificaciones técnicas que deben utilizarse en un esquema europeo de certificación de la ciberseguridad deben respetar los requisitos establecidos en el anexo II del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([19]). No obstante, podrían considerarse necesarias algunas variaciones con respecto a estos requisitos en casos debidamente justificados en los que dichas especificaciones técnicas vayan a utilizarse en un esquema europeo de certificación de la ciberseguridad de nivel de garantía «elevado». Los motivos que justifican tales variaciones deben hacerse públicos.

(77) La evaluación certificada de la conformidad es el procedimiento por el que se evalúa si se han cumplido los requisitos especificados en relación con un proceso, producto o servicio de TIC. Para llevar a cabo este procedimiento es necesario un tercero independiente, que no sea el fabricante del producto ni el proveedor del producto, servicio o proceso de TIC que está siendo evaluado. Un certificado europeo de ciberseguridad debe ser expedido tras un procedimiento de evaluación exitoso de un producto, servicio o proceso de TIC. Un certificado europeo de ciberseguridad debe considerarse una confirmación de que la evaluación se ha llevado a cabo de forma apropiada. En función del nivel de garantía, el esquema europeo de certificación de la ciberseguridad debe determinar si el encargado de expedir el certificado es un organismo público o privado.

La evaluación de la conformidad y la certificación no pueden garantizar por sí mismas la ciberseguridad de los productos, servicios y procesos de TIC certificados. Se trata más bien de un procedimiento y una metodología técnica que garantizan que los productos, servicios y procesos de TIC han sido sometidos a ensayo y cumplen determinados requisitos de ciberseguridad establecidos en otro lugar, por ejemplo en las normas técnicas.

(78) La elección del nivel adecuado de certificación y de los requisitos de seguridad asociados por parte de los usuarios de certificados europeos de ciberseguridad debe basarse en el análisis del riesgo asociado con el uso de productos, servicios o procesos de TIC. Por tanto, el nivel de garantía debe así reflejar el nivel de riesgo asociado con el uso previsto de un producto, servicio o proceso de TIC.

([19]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

(79) Un esquema europeo de certificación de la ciberseguridad podría determinar que la evaluación de la conformidad se realice bajo la responsabilidad exclusiva del fabricante o proveedor de productos, servicios y procesos de TIC (autoevaluación de la conformidad). En tales casos, basta con que el fabricante o proveedor de productos, servicios y procesos de TIC lleve a cabo por sí mismo todas las comprobaciones que garanticen la conformidad de los productos, servicios o procesos de TIC con el esquema de certificación europea de ciberseguridad. Este tipo de evaluación de la conformidad debe considerarse adecuado para productos, servicios o procesos de TIC poco complejos que presentan un nivel de riesgo bajo para el público, por ejemplo, cuando el diseño y el mecanismo de producción son sencillos. Asimismo, la autoevaluación de la conformidad debe estar permitida para los productos, servicios o procesos de TIC, únicamente cuando corresponden al nivel de garantía «básico».

(80) Un esquema europeo de certificación de la ciberseguridad puede permitir la autoevaluación de la conformidad y las certificaciones de los productos, servicios o procesos de TIC. En este caso, el esquema debe establecer medios claros y comprensibles para que los consumidores u otros usuarios puedan diferenciar los productos, servicios o procesos de TIC respecto de los cuales el fabricante o proveedor de productos, servicios o procesos de TIC es responsable de la evaluación, y los productos, servicios o procesos de TIC certificados por un tercero.

(81) El fabricante o proveedor de productos, servicios o procesos de TIC que lleve a cabo una autoevaluación de la conformidad debe redactar y firmar la declaración de conformidad de la UE como parte del procedimiento de evaluación de la conformidad. La declaración de conformidad de la UE es un documento que determina si un producto, servicio o proceso de TIC específico cumple los requisitos del esquema europeo de certificación de la ciberseguridad. Al expedir y firmar la declaración de conformidad de la UE, el fabricante o proveedor de productos, servicios o procesos de TIC asume la responsabilidad de que el producto, servicio o proceso de TIC cumple los requisitos legales del esquema europeo de certificación de la ciberseguridad. Debe presentarse una copia de la declaración de conformidad de la UE a la autoridad nacional de certificación de la ciberseguridad y a ENISA.

(82) Los fabricantes o proveedores de productos, servicios o procesos de TIC deben poner a disposición de la autoridad nacional de certificación de la seguridad competente, por un plazo previsto en el esquema europeo específico de certificación de la ciberseguridad, la declaración de conformidad de la UE, la documentación técnica, y toda la información pertinente relativa a la conformidad de los productos, servicios o procesos de TIC con el esquema europeo de certificación de la ciberseguridad de que se trate. La documentación técnica debe especificar los requisitos aplicables en virtud del esquema y debe contemplar, en la medida en que sea pertinente para la autoevaluación de la conformidad, el diseño, la fabricación y el funcionamiento del producto, servicio o proceso de TIC. La documentación técnica debe recopilarse de forma tal que permita la evaluación de la conformidad de un producto o servicio de TIC con los requisitos aplicables en virtud de dicho esquema.

(83) La gobernanza del marco europeo de certificación de la ciberseguridad tiene en cuenta la participación de los Estados miembros así como la participación adecuada de las partes interesadas y determina el papel de la Comisión en la planificación y la propuesta, la solicitud, la preparación, la adopción y la revisión de los esquemas europeos de certificación de la ciberseguridad.

(84) La Comisión debe elaborar, con el apoyo del Grupo Europeo de Certificación de la Ciberseguridad (GECC) y del Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad y tras una consulta abierta y amplia, un programa de trabajo evolutivo de la Unión para los esquemas europeos de certificación de la ciberseguridad y debe publicarlo en forma de instrumento no vinculante. El programa de trabajo evolutivo de la Unión debe constituir un documento estratégico que permita en particular a la industria, a las autoridades nacionales y a los organismos de normalización prepararse de antemano para los futuros esquemas europeos de certificación de la ciberseguridad.

El programa de trabajo evolutivo de la Unión debe incluir una perspectiva plurianual de las solicitudes de las propuestas de esquemas que la Comisión tenga intención de presentar a ENISA para su preparación, sobre la base de motivos específicos. La Comisión debe tener en cuenta este programa de trabajo evolutivo durante la elaboración de su plan evolutivo para la normalización de las TIC y de las peticiones de normalización dirigidas a los organismos europeos de normalización. Habida cuenta de la rapidez en la introducción y asimilación de las nuevas tecnologías, de la aparición de riesgos relacionados con la ciberseguridad anteriormente desconocidos o de la evolución de la legislación y de los mercados, la Comisión o el GECC debe estar facultado para solicitar a ENISA que prepare propuestas de esquemas que no se incluían en el programa de trabajo evolutivo de la Unión. En tales casos, la Comisión y el GECC también deben evaluar la necesidad de dicha solicitud teniendo presentes los fines y objetivos generales del presente Reglamento y garantizando la continuidad por lo que respecta a la planificación y el uso de recursos por ENISA.

Tras recibir una solicitud, ENISA debe preparar sin demora indebida propuestas de esquemas para productos, servicios o procesos de TIC específicos. La Comisión debe evaluar los efectos positivos y negativos de su solicitud en el mercado concreto de que se trate, en especial en las pymes, en la innovación, en los obstáculos a la entrada a dicho mercado y en los costes para los usuarios finales. A continuación, la Comisión, sobre la base de la propuesta de esquema presentada por ENISA, debe estar facultada para adoptar el esquema 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 esquemas 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 esquema concreto.

Entre ellos deben figurar el alcance y objeto de la certificación de la ciberseguridad, incluidas las categorías de productos, servicios y procesos 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 previsto («básico», «sustancial» o «elevado») y los niveles de evaluación cuando proceda. ENISA debe poder rechazar una solicitud del GECC. Corresponde al Consejo de Administración adoptar tales decisiones y deben estar debidamente motivadas.

(85) ENISA debe encargarse del mantenimiento de un sitio web que facilite información y publicidad sobre los esquemas europeos de certificación de la ciberseguridad, que debe incluir, entre otras cosas, las solicitudes para preparar una propuesta de esquema europeo de certificación de la ciberseguridad y los comentarios recibidos en el proceso de consulta llevado a cabo por ENISA en la fase de preparación. El sitio web también debe proporcionar información sobre los certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE expedidos en virtud del presente Reglamento, incluyendo información relativa a la retirada y expiración de dichos certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE. El sitio web debe indicar asimismo aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

(86) El nivel de garantía de un esquema europeo de certificación constituye la base para confiar en que un producto, servicio o proceso de TIC cumple los requisitos sobre seguridad de un esquema europeo de certificación de la ciberseguridad específico. Con el fin de garantizar la coherencia del marco europeo de certificación de la ciberseguridad, un esquema europeo de certificación de la ciberseguridad podría especificar niveles de garantía para los certificados europeos de ciberseguridad y las declaraciones de conformidad de la UE expedidos con arreglo a dicho esquema. Cada certificado europeo de ciberseguridad podría referirse a uno de los niveles de garantía («básico», «sustancial» o «elevado»), mientras que la declaración de conformidad de la UE solo podría referirse al nivel de garantía «básico». Los niveles de garantía deberían prever el rigor y la amplitud correspondientes para la evaluación del producto, servicio o proceso de TIC y deberían determinarse por referencia a especificaciones técnicas, normas y procedimientos relacionados, incluidos los controles técnicos, cuyo objetivo es reducir o evitar incidentes. Cada nivel de garantía debe ser coherente en los distintos ámbitos sectoriales a los que se aplica la certificación.

(87) Un esquema europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y lo exhaustivo de la metodología de evaluación utilizada. Los niveles de evaluación deben equivaler a uno de los niveles de garantía y deben asociarse con una combinación adecuada de componentes de garantía. En todos los niveles de garantía, el producto, servicio o proceso de TIC debe contener varias funciones de seguridad, definidas por el esquema, que pueden incluir una configuración innovadora segura, un código firmado, una actualización segura, la reducción de programas intrusos y la protección total de las memorias tanto de pila (*stack*) como de almacenamiento libre o dinámico (*heap*). Una vez creadas, dichas funciones deben conservarse utilizando fórmulas de desarrollo centradas en la seguridad e instrumentos asociados para garantizar que se incorporen mecanismos eficaces de forma fiable tanto programas informáticos como equipos informáticos.

(88) En el caso del nivel de garantía «básico», la evaluación debe regirse al menos por los siguientes componentes de garantía: la evaluación debe incluir como mínimo una revisión de la documentación técnica del producto, servicio o proceso de TIC por el organismo de evaluación de la conformidad. Cuando la certificación incluya procesos de TIC, también debe someterse a la revisión técnica el proceso utilizado para diseñar, desarrollar y mantener un producto o un servicio de TIC. En los casos en que un esquema europeo de certificación de la ciberseguridad establezca una autoevaluación de la conformidad, debe ser suficiente con que el fabricante o proveedor de los productos, servicios o procesos de TIC haya llevado a cabo una autoevaluación sobre el cumplimiento de los procesos, productos o servicios de TIC con respecto al esquema de certificación.

(89) En el caso del nivel de garantía «sustancial», la evaluación, además de cumplir con lo indicado para el nivel de garantía «básico», debe regirse al menos por la verificación del cumplimiento de las funcionalidades de seguridad del producto, servicio o proceso de TIC con respecto a su documentación técnica.

(90) Para el nivel de garantía «elevado», la evaluación, además de cumplir con lo indicado para el nivel de garantía «sustancial», debe regirse al menos por una prueba de eficacia que evalúe la resistencia de las funcionalidades de seguridad del producto, servicio o proceso de TIC frente a ciberataques complejos efectuados por personas que tienen habilidades y recursos significativos.

(91) El recurso a la certificación europea de la ciberseguridad y a la declaración de conformidad de la UE debe seguir siendo voluntario, salvo que se disponga otra cosa en el Derecho de la Unión o en el Derecho de los Estados miembros adoptado con arreglo al Derecho de la Unión. Puesto que el Derecho no está armonizado, los Estados miembros deben poder adoptar reglamentos técnicos nacionales que establezcan la certificación obligatoria en virtud de un esquema europeo de certificación de la ciberseguridad de conformidad con la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([20]). Los Estados miembros también pueden recurrir a la certificación europea de la ciberseguridad en el contexto de la contratación pública y de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([21]).

(92) Para mejorar el nivel de la ciberseguridad de algunos ámbitos en la Unión Europea, en el futuro podría revelarse necesario convertir en obligatorias para algunos productos, servicios o procesos de TIC, determinadas exigencias específicas en materia de ciberseguridad, así como la certificación relacionada con ella. La Comisión debe realizar de forma periódica un seguimiento de la incidencia de los esquemas de certificación adoptados sobre la disponibilidad en el mercado interior de productos, servicios y procesos de TIC seguros y evaluar periódicamente el grado de utilización de los esquemas de certificación para los fabricantes y proveedores de productos, servicios y procesos de TIC en la Unión. Sería conveniente analizar la eficacia de los esquemas europeos de certificación de la ciberseguridad y si determinados esquemas deben convertirse en obligatorios a la luz de la legislación de la Unión relativa a la ciberseguridad, en particular la Directiva (UE) 2016/1148, teniendo en cuenta la seguridad de las redes y los sistemas de información utilizados por los operadores de servicios esenciales.

(93) Los certificados europeos de la ciberseguridad y las declaraciones de conformidad de la UE deben ayudar a los usuarios finales a elegir con conocimiento de causa. Así pues, los productos, servicios y procesos de TIC que han sido certificados o para los que se ha expedido una declaración de conformidad de la UE deben ir acompañados de información estructurada, adaptada al nivel técnico previsto del usuario al que se destinan. Toda la información debe estar disponible en línea, y cuando proceda, podría estar disponible en formato físico. El usuario final debe poder tener acceso a informaciones relativas al número de referencia del esquema de certificación, al nivel de garantía, a la descripción de riesgos relacionados con la ciberseguridad asociados al producto, servicio o proceso de TIC, a la autoridad u organismo emisor, o debe poder obtener una copia del certificado europeo de ciberseguridad. Además, debe informarse al usuario final sobre la política de apoyo a la ciberseguridad (es decir, durante cuánto tiempo podrá el usuario final esperar recibir actualizaciones y correcciones de la ciberseguridad) del fabricante o del proveedor de productos, servicios o procesos de TIC. Cuando proceda, debe recibir orientaciones sobre las acciones o los ajustes que el usuario final podrá ejecutar para mantener o aumentar la ciberseguridad de productos, servicios o procesos de TIC, y ser informado sobre un punto de contacto único para comunicarse y recibir apoyo en caso de ciberataques (además de la comunicación automática). Dicha información debe actualizarse periódicamente y estar disponible en un sitio web que facilite información sobre los esquemas europeos de certificación de la ciberseguridad.

(94) Con vistas a alcanzar los objetivos del presente Reglamento y evitar la fragmentación del mercado interior, los esquemas o procedimientos nacionales de certificación de la ciberseguridad para productos, servicios o procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad deben dejar de surtir efecto a partir de una fecha establecida por la Comisión en el acto de ejecución. Además, los Estados miembros deben abstenerse de introducir nuevos esquemas nacionales de certificación de la ciberseguridad para productos, servicios o procesos de TIC cubiertos ya por un esquema europeo de certificación de la ciberseguridad existente. No obstante, no debe impedirse a los Estados miembros adoptar o conservar esquemas nacionales de certificación de la ciberseguridad con fines de seguridad nacional. Los Estados miembros deben comunicar a la Comisión y al GECC su intención de introducir nuevos esquemas nacionales de certificación de la ciberseguridad. La Comisión y el GECC deben evaluar el impacto del nuevo esquema nacional de certificación de la ciberseguridad sobre el correcto funcionamiento del mercado interior, y ponderar el posible interés estratégico de solicitar en su lugar un esquema europeo de certificación de la ciberseguridad.

(95) Los esquemas europeos de certificación de la ciberseguridad están destinados a ayudar a la armonización de las prácticas de ciberseguridad dentro de la Unión. Han de contribuir a aumentar el nivel de seguridad en el seno de la Unión. Además, cuando se conciban estos esquemas debe tenerse en cuenta y permitirse la introducción de innovaciones en materia de ciberseguridad.

([20]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (Texto pertinente a efectos del EEE) (DO L 241 de 17.9.2015, p. 1).

([21]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

(96) Los esquemas europeos de certificación de la ciberseguridad deben tener en cuenta los métodos actuales de desarrollo de programas informáticos y sus correspondientes equipos y, en especial, el impacto de las frecuentes actualizaciones de los programas informáticos o de los microprogramas incorporados sobre los certificados europeos de la ciberseguridad individuales. Los esquemas europeos de certificación de la ciberseguridad deben especificar las condiciones en que una actualización podrá exigir que un producto, servicio o proceso de TIC tenga que volver a ser certificado o que se reduzca el ámbito de un certificado europeo de la ciberseguridad específico, teniendo en cuenta cualquier posible efecto negativo de la actualización sobre la conformidad con los requisitos de seguridad del certificado.

(97) Una vez que se adopte un esquema europeo de certificación de la ciberseguridad, los fabricantes o proveedores de productos, servicios o procesos de TIC deben tener la posibilidad de presentar una solicitud de certificación de sus productos o servicios de TIC al organismo de evaluación de la conformidad que prefieran en cualquier parte de la Unión. Los organismos de evaluación de la conformidad deben ser acreditados por un organismo nacional de acreditación si cumplen determinados requisitos especificados en el presente Reglamento. La acreditación debe expedirse por un período máximo de cinco años y debe renovarse en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos. Los organismos nacionales de acreditación deben restringir, suspender o 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.

(98) Las referencias en la legislación nacional a normas nacionales que hayan dejado de producir efectos jurídicos debido a la entrada en vigor de un esquema europeo de certificación de la ciberseguridad pueden ser una fuente de confusión. Por consiguiente, los Estados miembros deben reflejar en sus legislaciones nacionales la adopción de un esquema europeo de certificación de la ciberseguridad.

(99) Para conseguir una equivalencia normativa en toda la Unión, facilitar el reconocimiento mutuo y favorecer la aceptación global de los certificados europeos de la ciberseguridad y declaraciones de conformidad de la UE, es necesario poner a punto un sistema de evaluación interpares entre las autoridades nacionales de certificación de la ciberseguridad. Dicha evaluación interpares debe abarcar la conformidad de los procedimientos de supervisión de los productos, servicios y procesos de TIC con los correspondientes certificados europeos de la ciberseguridad, de vigilancia del respeto de las obligaciones de los fabricantes o de los proveedores de los productos, servicios y procesos de TIC que realizan una autoevaluación de la conformidad y de vigilancia de la conformidad de los organismos de evaluación, así como la adecuación de los conocimientos especializados del personal de los organismos que expiden los certificados para niveles de garantía «elevados». La Comisión, mediante un acto de ejecución, debe poder establecer al menos un plan quinquenal para la evaluación interpares, además de fijar los criterios y métodos de funcionamiento de dicho sistema de evaluación interpares.

(100) Sin perjuicio del sistema general de evaluación interpares que se establezca entre todas las autoridades nacionales de certificación de la ciberseguridad en relación con el marco de certificación europea de la ciberseguridad, determinados esquemas de certificación europea de la ciberseguridad pueden incluir un mecanismo de evaluación interpares para aquellos organismos que expidan certificados europeos de ciberseguridad de los productos, servicios y procesos de TIC con un nivel de garantía «elevado» en aplicación de dichos esquemas. El GECC debe apoyar la aplicación de dichos mecanismos de evaluación interpares. Dichas evaluaciones interpares deben establecer en particular si los organismos de que se trate desempeñan sus cometidos de forma armonizada y pueden incluir vías de recurso. Los resultados de las evaluaciones interpares deben hacerse públicos. Estos organismos pueden adoptar las medidas apropiadas para adaptar sus prácticas y sus conocimientos especializados en consecuencia.

(101) Los Estados miembros deben designar a una o más autoridades nacionales de certificación de la ciberseguridad para supervisar el cumplimiento de las obligaciones derivadas del presente Reglamento. Una autoridad nacional de certificación de la ciberseguridad puede ser una existente o una nueva autoridad. Asimismo, un Estado miembro debe poder designar, previo acuerdo con otro Estado miembro, a una o más autoridades nacionales de certificación de la ciberseguridad en el territorio de ese otro Estado miembro.

(102) En particular, las autoridades nacionales de certificación de la ciberseguridad deben supervisar y hacer cumplir las obligaciones de los fabricantes o proveedores de productos, servicios o procesos de TIC establecidos en sus territorios respectivos en relación con la declaración de conformidad de la UE, asistir a los organismos de acreditación nacionales en el proceso de seguimiento y supervisión de las actividades de los organismos de evaluación de la conformidad facilitándoles conocimientos especializados e información pertinente, autorizar a los organismos de evaluación de la conformidad a desempeñar sus funciones cuando cumplen los requisitos adicionales establecidos en un esquema europeo de certificación de la ciberseguridad y hacer el seguimiento de la correspondiente evolución en el ámbito de la certificación de la ciberseguridad. Las autoridades nacionales de certificación de la ciberseguridad deben tramitar las reclamaciones presentadas por personas físicas o jurídicas en

relación con los certificados europeos de la ciberseguridad expedidos por ellas o en relación con los certificados europeos de la ciberseguridad expedidos por los organismos de evaluación de la conformidad, cuando dichos certificados se refieran al nivel de garantía «elevado», deben 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, las autoridades nacionales de certificación de la ciberseguridad deben cooperar con otras autoridades nacionales de certificación de la ciberseguridad u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos, servicios y procesos de TIC que no se ajusten a los requisitos del presente Reglamento o de esquemas europeos de certificación de la ciberseguridad específicos. La Comisión debe facilitar ese intercambio de información poniendo a disposición un sistema electrónico general de apoyo a la información, por ejemplo, el sistema de información y comunicación para la vigilancia del mercado (siglas inglesas ICSMS) o el sistema de alerta rápida para productos peligrosos no alimenticios (RAPEX), ya utilizados por las autoridades de vigilancia del mercado en virtud del Reglamento (CE) n.º 765/2008.

(103) Con vistas a garantizar la aplicación coherente del marco europeo de certificación de la ciberseguridad, debe establecerse un GECC, constituido por representantes de las autoridades nacionales de certificación de la ciberseguridad u otras autoridades nacionales pertinentes. Los cometidos principales del GECC 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 ENISA en la preparación de las propuestas de esquemas de certificación de la ciberseguridad, en casos debidamente justificados solicitar a ENISA que prepare una propuesta de esquema, y adoptar dictámenes dirigidos a ENISA sobre propuestas de esquemas y adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los esquemas europeos de certificación de la ciberseguridad existentes. El GECC debe facilitar el intercambio de buenas prácticas y conocimientos especializados entre las diferentes autoridades nacionales de certificación de la ciberseguridad responsables de la autorización de los organismos de evaluación de la conformidad y la expedición de certificados europeos de la ciberseguridad.

(104) Con el fin de reforzar la sensibilización y facilitar la aceptación de los futuros esquemas europeos de certificación de ciberseguridad, la Comisión puede 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, servicios y procesos TIC certificados.

(105) Con el fin de seguir facilitando el comercio y reconociendo que las cadenas de suministro de TIC son mundiales, la Unión, de conformidad con el artículo 218 del Tratado de Funcionamiento de la Unión Europea (TFUE), puede celebrar acuerdos de reconocimiento mutuo relativos a certificados europeos de ciberseguridad. La Comisión, teniendo en cuenta el asesoramiento de ENISA y del GECC, puede recomendar que se inicien las negociaciones correspondientes. Cada esquema europeo de certificación de la ciberseguridad debe proporcionar condiciones específicas para dichos acuerdos de reconocimiento mutuo con terceros países.

(106) A fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([22]).

(107) Debe utilizarse el procedimiento de examen para la adopción de los actos de ejecución sobre los esquemas europeos de certificación de la ciberseguridad de productos, servicios o procesos de TIC, para la adopción de los actos de ejecución sobre las disposiciones de ejecución de las investigaciones por parte de ENISA; para la adopción de los actos de ejecución sobre un plan para la revisión interpares de las autoridades nacionales de certificación de la ciberseguridad y para la adopción de los actos de ejecución 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 certificación de la ciberseguridad.

(108) Las actividades de ENISA deben evaluarse de modo periódico e independiente. La evaluación debe tener en cuenta el logro de sus objetivos por parte de ENISA, sus prácticas de trabajo y la pertinencia de sus tareas, en particular sus tareas relativas a la cooperación operativa a nivel de la Unión. La evaluación también debe valorar el impacto, eficacia y eficiencia del marco europeo de certificación de la ciberseguridad. En caso de procederse a una revisión, la Comisión debe evaluar el modo de reforzar el papel de ENISA como punto de referencia en materia de asesoramiento y conocimiento especializado y debe también evaluar que se encomiende a ENISA el cometido de apoyar la evaluación de los productos, servicios y procesos de TIC de terceros países que no cumplan las normas de la Unión, cuando dichos productos, servicios y procesos entren en la Unión.

([22]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(109) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

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

HAN ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

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

a) los objetivos, tareas y aspectos organizativos relativos a ENISA (Agencia de la Unión Europea para la Ciberseguridad), y

b) un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

El marco a que se refiere el párrafo primero, letra b), se aplicará sin perjuicio de las disposiciones específicas contenidas en otros actos jurídicos de la Unión relativas a la certificación de carácter voluntario u obligatorio.

2. El presente Reglamento se entenderá sin perjuicio de las competencias de los Estados miembros en materia de actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

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

2) «redes y sistemas de información»: las redes y sistemas de información según se definen en el artículo 4, punto 1, de la Directiva (UE) 2016/1148;

3) «estrategia nacional de seguridad de las redes y sistemas de información»: una estrategia nacional de seguridad de las redes y sistemas de información según se define en el artículo 4, punto 3, de la Directiva (UE) 2016/1148;

4) «operador de servicios esenciales»: un operador de servicios esenciales según se define en el artículo 4, punto 4, de la Directiva (UE) 2016/1148;

5) «proveedor de servicios digitales»: un proveedor de servicios digitales según se define en el artículo 4, punto 6, de la Directiva (UE) 2016/1148;

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

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

8) «ciberamenaza»: cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas;

9) «esquema europeo de certificación de la ciberseguridad»: conjunto completo, de disposiciones, requisitos técnicos, normas y procedimientos establecidos a escala de la Unión y que se aplican a la certificación o a la evaluación de la conformidad de los productos, servicios y procesos de TIC específicos;

10) «esquema nacional de certificación de la ciberseguridad»: conjunto completo de disposiciones, requisitos técnicos, normas y procedimientos desarrollados y adoptados por una autoridad pública nacional, y que se aplican a la certificación o a la evaluación de la conformidad de los productos, servicios y procesos de TIC incluidos en el ámbito de aplicación de dicho esquema específico;

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

12) «producto de TIC»: un elemento o un grupo de elementos de las redes y los sistemas de información;

13) «servicio de TIC»: un servicio que consista, en su totalidad o principalmente, en la transmisión, almacenamiento, extracción o tratamiento de información mediante redes y sistemas de información;

14) «proceso de TIC»: un conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio de TIC;

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

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

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

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

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

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

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

22) «autoevaluación de la conformidad»: una acción realizada por un fabricante o un proveedor de productos, servicios o procesos de TIC que evalúa el cumplimiento por estos de los requisitos establecidos en el esquema europeo de certificación de la ciberseguridad específico.

TÍTULO II

ENISA (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD)

CAPÍTULO I

Mandato y objetivos

Artículo 3

Mandato

1. ENISA desempeñará el cometido que le asigna el presente Reglamento con el fin de lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros, a las instituciones, órganos y organismos de la Unión en la mejora de la ciberseguridad. ENISA actuará como punto de referencia de asesoramiento y conocimientos especializados en cuestiones relacionadas con la ciberseguridad para las instituciones, órganos y organismos de la Unión, así como para otras partes interesadas pertinentes de la Unión.

Al desempeñar las tareas que le asigna el presente Reglamento, ENISA contribuirá a reducir la fragmentación del mercado interior.

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

3. Al desempeñar sus funciones, ENISA actuará con independencia, evitando la duplicación con las actividades de los Estados miembros y teniendo en cuenta los conocimientos ya existentes de los Estados miembros.

4. ENISA desarrollará sus recursos propios, en particular las capacidades y las competencias humanas y técnicas, necesarios para desarrollar las tareas que le asigna el presente Reglamento.

Artículo 4

Objetivos

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

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

3. ENISA prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros y las partes interesadas públicas y privadas a fin de incrementar la protección de sus redes y sistemas de información, desarrollar y mejorar la ciberresiliencia y la capacidad de respuesta y desarrollar las capacidades y competencias en el ámbito de la ciberseguridad.

4. ENISA fomentará la cooperación, en particular el intercambio de información, y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, públicas y privadas, sobre las cuestiones relacionadas con la ciberseguridad.

5. ENISA contribuirá a incrementar las capacidades de ciberseguridad a nivel de la Unión para apoyar las acciones de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

6. ENISA promoverá el uso de la certificación europea de ciberseguridad, con vistas a evitar la fragmentación del mercado interior. ENISA contribuirá a la creación y al mantenimiento de un marco de certificación europea de la ciberseguridad de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos, servicios y procesos de TIC y reforzar así la confianza en el mercado interior digital y su competitividad.

7. ENISA promoverá un alto nivel de sensibilización sobre ciberseguridad, en particular ciberhigiene y ciberalfabetización de los ciudadanos, organizaciones y empresas.

CAPÍTULO II

Tareas

Artículo 5

Elaboración y ejecución de la política y del Derecho de la Unión

ENISA contribuirá a la elaboración y ejecución de la política y del Derecho de la Unión:

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

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

3. Asistiendo a los Estados miembros y a las instituciones, órganos y organismos de la Unión para que elaboren y promuevan políticas de ciberseguridad que apoyen la disponibilidad general y la integridad del núcleo público de la internet abierta.

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

5. Respaldando:

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

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

   c) la asistencia a los Estados miembros en la ejecución de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de los datos y la privacidad, así como la emisión, previa solicitud, de un dictamen para el Comité Europeo de Protección de Datos.

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

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

   b) el resumen de las notificaciones de violación de la seguridad y pérdida de la integridad respecto de los proveedores de servicios de confianza, transmitidas por los organismos de supervisión a ENISA, de conformidad con el artículo 19, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([23]);

   c) las notificaciones de incidentes relacionados con la seguridad transmitidas por los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, transmitidas por las autoridades competentes a ENISA, de conformidad con el artículo 40 de la Directiva (UE) 2018/1972.

([23]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

Artículo 6

Creación de capacidades

1. ENISA asistirá:

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

b) con carácter voluntario, a los Estados miembros y las instituciones, órganos y organismos de la Unión en el establecimiento y la aplicación de políticas de divulgación de vulnerabilidades;

c) a las instituciones, órganos y organismos de la Unión en sus esfuerzos para mejorar la prevención, detección, análisis de ciberamenazas e incidentes y para mejorar su capacidad de respuesta a dichas ciberamenazas e incidentes, en particular a través de un apoyo adecuado al CERT;

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

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

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

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

h) a los Estados miembros, organizando periódicamente ejercicios de ciberseguridad a escala de la Unión a que se refiere el artículo 7, apartado 5, y ello al menos cada dos años, y formulando recomendaciones políticas basadas en el proceso de evaluación de los ejercicios y en las enseñanzas extraídas de ellos;

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

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

2. ENISA apoyará la puesta en común de información dentro de los sectores y entre ellos, en particular en los sectores que figuran en el anexo II de la Directiva (UE) 2016/1148, aportando mejores prácticas y orientaciones sobre las herramientas disponibles, el procedimiento y la manera de abordar los asuntos normativos relacionados con el intercambio de información.

Artículo 7

Cooperación operativa a nivel de la Unión

1. ENISA apoyará la cooperación operativa entre los Estados miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas.

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

a) el intercambio de conocimientos técnicos y mejores prácticas;

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

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

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

4. ENISA apoyará a los Estados miembros en lo relativo a la cooperación operativa dentro de la red de CSIRT:

a) asesorando sobre cómo mejorar su capacidad para prevenir, detectar y dar respuesta a los incidentes y, previa solicitud de uno o varios Estados miembros, proporcionando asesoramiento sobre una amenaza específica;

b) prestando asistencia, previa solicitud de uno o varios Estados miembros, en la evaluación de los incidentes con un impacto significativo o sustancial, proporcionando conocimientos técnicos y facilitando la gestión técnica de dichos incidentes, en particular apoyando el intercambio voluntario de información pertinente y soluciones técnicas entre Estados miembros;

c) analizando las vulnerabilidades e incidentes sobre la base de la información públicamente disponible o la información que los Estados miembros faciliten voluntariamente para este fin, y

d) previa solicitud de uno o varios Estados miembros, dando apoyo en las investigaciones técnicas *ex post* de los incidentes que tengan un impacto significativo o sustancial en el sentido de la Directiva (UE) 2016/1148.

En el desempeño de estas tareas, ENISA y el CERT-UE entablarán una cooperación estructurada con el fin de beneficiarse de las sinergias y evitar la duplicación de actividades.

5. ENISA organizará regularmente ejercicios de ciberseguridad a nivel de la Unión y apoyará a los Estados miembros y a las instituciones, órganos y organismos de la Unión en la organización de ejercicios de ciberseguridad a petición suya. Dichos ejercicios de ciberseguridad a nivel de la Unión podrán constar de elementos técnicos, operativos o estratégicos. Cada dos años, ENISA organizará un ejercicio global a gran escala.

En su caso, ENISA participará asimismo en la realización de ejercicios sectoriales de ciberseguridad, y contribuirá a organizarlos cuando proceda, junto con organizaciones competentes que también participen en los ejercicios de ciberseguridad a escala de la Unión.

6. ENISA, en estrecha colaboración con los Estados miembros, elaborará un informe periódico y detallado sobre la situación técnica de la ciberseguridad en la UE, relativo a incidentes y ciberamenazas, basándose en la información disponible al público, en su propio análisis y en los informes comunicados, entre otros, por los CSIRT de los Estados miembros o los puntos de contacto únicos de la Directiva (UE) 2016/1148, ambos con carácter voluntario; el EC3 y el CERT-UE.

7. ENISA contribuirá a la elaboración de una respuesta cooperativa, a nivel de la Unión y de los Estados miembros, a los incidentes o crisis transfronterizos a gran escala relacionados con la ciberseguridad, principalmente por los siguientes medios:

a) agregación y análisis de los informes procedentes de fuentes nacionales que son de dominio público y han sido puestos en común de manera voluntaria, con vistas a contribuir a la creación de una perspectiva común de la situación;

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

c) facilitación, previa petición, de la gestión técnica de tales incidentes o crisis, en particular apoyando la puesta en común voluntaria de soluciones técnicas entre los Estados miembros;

d) apoyo a las instituciones, órganos y organismos de la Unión y, previa petición, a los Estados miembros en la comunicación pública en torno a esos incidentes o crisis;

e) prueba de los planes de cooperación para responder a dichos incidentes o crisis a nivel de la Unión y apoyo, previa petición, a los Estados miembros para que prueben dichos planes a escala nacional.

Artículo 8

Mercado, certificación de la ciberseguridad y normalización

1. ENISA apoyará y promoverá el desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de, productos, servicios y procesos de TIC, según lo establecido en el título III del presente Reglamento, por los siguientes medios:

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

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

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

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

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

2. ENISA se encargará de la secretaría del Grupo de las Partes Interesadas de Certificación de la Ciberseguridad de conformidad con el artículo 22, del apartado 4.

3. ENISA recopilará y publicará directrices y desarrollar buenas prácticas, relativas a los requisitos de ciberseguridad de los productos, servicios y procesos de TIC, en cooperación con las autoridades nacionales de certificación de la ciberseguridad y con la industria, de una manera formal, estructurada y transparente.

4. ENISA contribuirá a un refuerzo de capacidades relacionada con los procesos de evaluación y certificación, recopilando y publicando directrices y proporcionando apoyo a los Estados miembros, a instancia de estos.

5. ENISA facilitará el establecimiento y la adopción de normas europeas e internacionales para la gestión de riesgos y para la seguridad de los productos, servicios y procesos de TIC.

6. ENISA elaborará, en colaboración con los Estados miembros y la industria, directrices y orientaciones relativas a las áreas técnicas relacionadas con los requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, así como relativas a normas ya existentes, entre ellas las normas nacionales de los Estados miembros, en virtud del artículo 19, apartado 2, de la Directiva (UE) 2016/1148.

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

Artículo 9

Conocimiento e información

ENISA:

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

b) realizará análisis estratégicos a largo plazo de las ciberamenazas e incidentes con el fin de detectar las tendencias emergentes y ayudar a prevenir los incidentes;

c) en cooperación con los expertos de las autoridades de los Estados miembros y las partes interesadas pertinentes, emitirá dictámenes, orientaciones y mejores prácticas para la seguridad de las redes y los sistemas de información, en particular en el ámbito de la seguridad de las infraestructuras que sustentan los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148 y las utilizadas por los proveedores de servicios digitales enumerados en el anexo III de dicha Directiva;

d) reunirá, organizará y pondrá a disposición del público, a través de un portal asignado a este propósito, información sobre la ciberseguridad facilitada por las instituciones, órganos y organismos de la Unión y, de manera voluntaria, por los Estados miembros y las partes interesadas de los sectores público y privado;

e) recopilará y analizará la información disponible públicamente relativa a incidentes significativos y elaborará informes con el fin de ofrecer orientaciones a los ciudadanos, organizaciones y empresas de toda la Unión.

Artículo 10

Sensibilización y educación

ENISA:

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

b) en cooperación con los Estados miembros, y las instituciones, órganos y organismos de la Unión y con la industria, organizará campañas periódicas de divulgación para aumentar la ciberseguridad y su visibilidad en la Unión y fomentará un amplio debate público;

c) asistirá a los Estados miembros en sus esfuerzos para sensibilizar sobre la ciberseguridad y promover la formación en este ámbito;

d) apoyará una mejor coordinación y el intercambio de mejores prácticas entre Estados miembros sobre sensibilización y educación en materia de ciberseguridad.

Artículo 11

Investigación e innovación

En relación con la investigación y la innovación, ENISA:

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

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

c) contribuirá a la agenda estratégica de investigación e innovación a escala de la Unión en el ámbito de la ciberseguridad.

Artículo 12

Cooperación internacional

ENISA contribuirá a los esfuerzos de la Unión por cooperar con terceros países y organizaciones internacionales, así como dentro de los marcos de cooperación internacional pertinentes, a fin de promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad, por los siguientes medios:

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

b) facilitar, a petición de la Comisión, el intercambio de mejores prácticas;

c) facilitar asesoramiento especializado a la Comisión cuando así se solicite;

d) facilitar asesoramiento y apoyo a la Comisión en materia de acuerdos de reconocimiento mutuo de certificados de ciberseguridad con terceros países en colaboración con el GECC creado en virtud del artículo 62.

CAPÍTULO III

Organización de ENISA

Artículo 13

Estructura de ENISA

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

a) un Consejo de Administración;

b) un Comité Ejecutivo;

c) un director ejecutivo;

d) un Grupo Consultivo de ENISA;

e) una red de funcionarios de enlace nacionales.

Sección 1

Consejo De Administración

Artículo 14

Composición del Consejo de Administración

1. El Consejo de Administración estará compuesto por un miembro nombrado por cada Estado miembro y dos miembros nombrados por la Comisión. Todos los miembros tendrán derecho a voto.

2. Cada miembro del Consejo de Administración tendrá un suplente. Dicho suplente representará al miembro en su ausencia.

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

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

Artículo 15

Funciones del Consejo de Administración

1. El Consejo de Administración:

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

b) adoptará el proyecto de documento único de programación de ENISA a que se refiere el artículo 24 antes de someterlo al dictamen de la Comisión;

c) adoptará, el documento único de programación de ENISA por una mayoría de dos tercios de sus miembros teniendo en cuenta el dictamen de la Comisión;

d) supervisará la aplicación de la programación anual y plurianual que figura en el documento único de programación;

e) adoptará el presupuesto anual de ENISA y ejercerá otras funciones relacionadas con el presupuesto de ENISA de conformidad con el capítulo IV;

f) evaluará y adoptará el informe anual consolidado sobre las actividades de ENISA, que incluirá las cuentas y describirá en qué medida ENISA ha cumplido sus indicadores de rendimiento y, a más tardar el 1 de julio del año siguiente, remitirá dicho informe, junto con su evaluación, al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas, y lo publicará;

g) adoptará las normas financieras aplicables a ENISA de conformidad con el artículo 32;

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

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

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

k) adoptará su propio reglamento interno, incluidas las normas relativas a las decisiones provisionales sobre la delegación de las tareas específicas con arreglo a lo dispuesto en el artículo 19, apartado 7;

l) ejercerá, respecto del personal de ENISA, las competencias atribuidas por el Estatuto de los funcionarios de la Unión Europea (en lo sucesivo, «Estatuto de los funcionarios») y las atribuidas por el Régimen aplicable a los otros agentes de la Unión Europea (en lo sucesivo, «Régimen aplicable a los otros agentes») establecidas por el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo ([24]) a la autoridad facultada para proceder a los nombramientos y a la autoridad facultada para proceder a las contrataciones (en lo sucesivo, «competencias de la autoridad facultada para proceder a los nombramientos») conforme al apartado 2;

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

n nombrará al director ejecutivo y, cuando proceda, ampliará su mandato o lo cesará de conformidad con el artículo 36;

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

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

q) autorizará el establecimiento de convenios de trabajo de conformidad en relación con el artículo 7;

r) autorizará el establecimiento y la celebración de convenios de trabajo de conformidad con el artículo 42.

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

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

3. Cuando así lo exijan circunstancias excepcionales, el Consejo de Administración podrá adoptar una decisión para suspender temporalmente la delegación de las competencias de la Autoridad facultada para proceder a los nombramientos en el director ejecutivo y la subdelegación de competencias por parte de este último, y ejercer él mismo las competencias o delegarlas en uno de sus miembros o en un miembro del personal distinto del director ejecutivo.

Artículo 16

Presidente del Consejo de Administración

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

Artículo 17

Reuniones del Consejo de Administración

1. Las reuniones del Consejo de Administración serán convocadas por su presidente.

2. El Consejo de Administración se reunirá al menos dos veces al año en sesión ordinaria. Celebrará también sesiones extraordinarias a instancias del presidente, de la Comisión o de como mínimo un tercio de sus miembros.

3. El director ejecutivo asistirá, sin tener derecho a voto, a las reuniones del Consejo de Administración.

4. Los miembros del Grupo Consultivo de ENISA del sector podrán participar, previa invitación del presidente, en las reuniones del Consejo de Administración, sin derecho a voto.

5. Los miembros del Consejo de Administración y sus suplentes podrán estar asistidos en las reuniones del Consejo de Administración por asesores o expertos, con sujeción al reglamento interno del Consejo de Administración.

6. ENISA se encargará de la secretaría del Consejo de Administración.

Artículo 18

Votaciones en el Consejo de Administración

1. El Consejo de Administración tomará sus decisiones por mayoría de sus miembros.

2. Se requerirá una mayoría de dos tercios de todos los miembros del Consejo de Administración para aprobar el documento único de programación, el presupuesto anual y el nombramiento, prórroga del mandato o cese del director ejecutivo.

3. Cada miembro dispondrá de un voto. En ausencia de un miembro, su suplente podrá ejercer el derecho a voto del miembro.

4. El presidente del Consejo de Administración participará en las votaciones.

5. El director ejecutivo no participará en las votaciones.

6. El reglamento interno del Consejo de Administración establecerá de manera más pormenorizada el régimen de votación, en particular las condiciones en las que un miembro puede actuar por cuenta de otro.

Sección 2

Comité Ejecutivo

Artículo 19

Comité Ejecutivo

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

2. El Comité Ejecutivo:

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

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

c) sin perjuicio de las responsabilidades del director ejecutivo establecidas en el artículo 20, le asistirá y asesorará en la aplicación de las decisiones del Consejo de Administración en cuestiones administrativas y presupuestarias con arreglo al artículo 20.

3. El Comité Ejecutivo estará formado por cinco miembros. Los miembros del Comité Ejecutivo serán escogidos entre los miembros del Consejo de Administración. Uno de los miembros será el presidente del Consejo de Administración, que también podrá presidir el Comité Ejecutivo, y otro será uno de los representantes de la Comisión. Los nombramientos de los miembros del Comité Ejecutivo tratarán de alcanzar una representación de género equilibrada en el Comité Ejecutivo. El director ejecutivo participará en las reuniones del Comité Ejecutivo, pero no tendrá derecho de voto.

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

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

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

7. Cuando sea necesario, por motivos de urgencia, el Comité Ejecutivo podrá adoptar determinadas decisiones provisionales en nombre del Consejo de Administración, en particular en materia de gestión administrativa, incluida la suspensión de la delegación de las competencias atribuidas a la autoridad facultada para proceder a los nombramientos, y para cuestiones presupuestarias. Dichas decisiones provisionales serán comunicadas sin demora indebida al Consejo de Administración, que decidirá si la aprueba o la rechaza a más tardar tres meses después de que se haya tomado la decisión. El Comité Ejecutivo no tomará una decisión en nombre del Consejo de Administración que deba ser aprobada por una mayoría de dos tercios del Consejo de Administración.

Sección 3

Director Ejecutivo

Artículo 20

Funciones del director ejecutivo

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

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

3. El director ejecutivo será responsable de:

a) la administración ordinaria de ENISA;

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

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

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

e) preparar el informe anual consolidado sobre las actividades de ENISA, en particular la aplicación del programa de trabajo anual, y presentarlo al Consejo de Administración para su evaluación y aprobación;

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

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

h) preparar el proyecto de normas financieras aplicables a ENISA a que se refiere el artículo 32;

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

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

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

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

m) intercambiar pareceres e información regularmente con las instituciones, órganos y organismos de la Unión sobre sus actividades en materia de ciberseguridad para garantizar la coherencia en la elaboración y ejecución de la política de la Unión;

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

4. Siempre que sea necesario y esté dentro del mandato de ENISA, y de conformidad con sus objetivos y tareas, el director ejecutivo podrá crear grupos de trabajo *ad hoc* integrados por expertos, incluidos expertos procedentes de las autoridades competentes de los Estados miembros. El director ejecutivo informará de ello anticipadamente al Consejo de Administración. Los procedimientos, en particular en lo que se refiere a la composición de los grupos de trabajo, el nombramiento de los expertos de dichos grupos por el director ejecutivo y el funcionamiento de los grupos de trabajo, se especificarán en el reglamento operativo interno de ENISA.

5. Cuando sea necesario, con el fin de desempeñar las funciones de ENISA de manera eficiente y eficaz y sobre la base de un análisis adecuado de los costes y los beneficios, el director ejecutivo podrá decidir establecer una o más oficinas locales en uno o más Estados miembros. Antes de tomar la decisión de establecer una oficina local, el director ejecutivo pedirá la opinión del Estado o Estados miembros afectados, en particular del Estado miembro donde se encuentra la sede de ENISA, y habrá de obtener el consentimiento previo de la Comisión y del Consejo de Administración. En caso de desacuerdo durante el proceso de consulta entre el director ejecutivo y los Estados miembros afectados, el asunto será debatido en el Consejo. El número agregado de efectivos en todas las oficinas locales se mantendrá en un mínimo y no superará el 40 % del total del personal de ENISA ubicado en el Estado miembro donde se encuentra la sede de ENISA. El número de efectivos en cada oficina local no superará el 10 % del total del personal de ENISA ubicado en el Estado miembro donde se encuentra la sede de ENISA.

Esta decisión especificará el alcance de las actividades que se llevarán a cabo en la oficina local, evitándose costes innecesarios y la duplicación de funciones administrativas de ENISA.

Sección 4

Grupo Consultivo de ENISA, Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad y red de funcionarios de enlace nacionales

Artículo 21

Grupo consultivo de ENISA

1. El Consejo de Administración establecerá de manera transparente, a propuesta del director ejecutivo, el Grupo Consultivo de ENISA compuesto por expertos reconocidos que representen a las partes interesadas pertinentes, tales como la industria de las TIC, los proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, las pymes, los operadores de servicios esenciales, los grupos de consumidores, los expertos académicos en ciberseguridad y los representantes de las autoridades competentes notificadas de conformidad con la Directiva (UE) 2018/1972, las organizaciones europeas de normalización y las autoridades encargadas de hacer cumplir la ley y de supervisar la protección de datos. El Consejo de Administración velará por que haya una participación equilibrada entre hombres y mujeres y un equilibrio geográfico, así como un equilibrio entre los distintos grupos de partes interesadas.

2. Los procedimientos del Grupo Consultivo de ENISA, en particular con respecto a su composición, la propuesta por el director ejecutivo a que se refiere el apartado 1, el número y nombramiento de sus miembros y el funcionamiento del Grupo Consultivo ENISA, se especificarán en el reglamento operativo interno de ENISA y se harán públicos.

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

4. El mandato de los miembros del Grupo Consultivo de ENISA tendrá una duración de dos años y medio. Los miembros del Consejo de Administración no podrán ser miembros del Grupo Consultivo de ENISA. Los expertos de la Comisión y de los Estados miembros podrán asistir a las reuniones del Grupo Consultivo de ENISA y participar en sus trabajos. Se podrá invitar a asistir a las reuniones del Grupo Consultivo de ENISA y a participar en sus trabajos a representantes de otros órganos que no sean miembros del Grupo cuando el director ejecutivo lo considere pertinente.

5. El Grupo Consultivo de ENISA asesorará a ENISA en lo relativo a la realización de sus actividades, a excepción de la aplicación de las disposiciones del título III del presente Reglamento. En particular, asesorará al director ejecutivo en la elaboración de una propuesta de programa de trabajo anual de ENISA y en el mantenimiento de la comunicación con las partes interesadas pertinentes sobre los aspectos relativos al programa de trabajo.

6. El Grupo Consultivo de ENISA informará periódicamente al Consejo de Administración de sus actividades.

Artículo 22

Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad

1. Se establecerá el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad.

2. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad estará compuesto por miembros seleccionados de entre expertos reconocidos que representen a las partes interesadas pertinentes. La Comisión, tras una convocatoria transparente y abierta, seleccionará, con base en una propuesta de ENISA, a los miembros del Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad velando por una participación equilibrada entre distintos grupos de partes interesadas, así como entre hombres y mujeres y un equilibrio geográfico.

3. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad desempeñará las siguientes tareas:

a) asesorar a la Comisión sobre cuestiones estratégicas relativas al marco europeo de certificación de la ciberseguridad;

b) asesorar a ENISA, previa solicitud, sobre cuestiones generales y estratégicas relativas a los cometidos de ENISA en relación con el mercado, la certificación de la ciberseguridad y la normalización;

c) prestar asistencia a la Comisión en la elaboración del programa de trabajo evolutivo de la Unión previsto en el artículo 47;

d) emitir un dictamen sobre el programa de trabajo evolutivo de la Unión con arreglo al artículo 47, apartado 4, y

e) en situaciones urgentes, prestar asesoramiento a la Comisión y al GECC sobre la necesidad de contar con esquemas de certificación adicionales no incluidos en el programa de trabajo evolutivo de la Unión, según lo previsto en los artículos 47y 48.

4. El Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad estará copresidido por los representantes de la Comisión y de ENISA, y su secretaría correrá a cargo de ENISA.

Artículo 23

Red de funcionarios de enlace nacionales

1. El Consejo de Administración, a propuesta del director ejecutivo, establecerá una red de funcionarios de enlace nacionales, compuesta por representantes de todos los Estados miembros (en lo sucesivo, «funcionarios de enlace nacionales»). Cada Estado miembro nombrará a un representante de la Red de funcionarios de enlace nacionales.

Las reuniones de la red de funcionarios de enlace nacionales podrán celebrarse en distintas formaciones de expertos.

2. En particular, la red de funcionarios de enlace nacionales facilitará el intercambio de información entre ENISA y los Estados miembros y apoyará a ENISA en la difusión de sus actividades, conclusiones y recomendaciones a las partes interesadas pertinentes en toda la Unión.

3. Los funcionarios de enlace nacionales actuarán como punto central de contacto a nivel nacional para facilitar la cooperación entre ENISA y los expertos nacionales en el contexto de la ejecución del programa de trabajo anual de ENISA.

4. Aunque los funcionarios de enlace nacionales trabajarán en estrecha cooperación con los representantes del Consejo de Administración de sus respectivos Estados miembros, la red de funcionarios de enlace nacionales en sí misma no duplicará el trabajo del Consejo de Administración ni de otros foros de la Unión.

5. Las funciones y los procedimientos de la red de funcionarios de enlace nacionales se especificarán en las normas internas de funcionamiento de ENISA y se harán públicos.

Sección 5

Funcionamiento

Artículo 24

Documento único de programación

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

2. Cada año, el director ejecutivo elaborará un proyecto de documento único de programación que contendrá la programación anual y plurianual, con la planificación de los recursos humanos y financieros correspondientes, de conformidad con el artículo 32 del Reglamento Delegado (UE) n.º 1271/2013 de la Comisión ([25]) y habida cuenta de las directrices establecidas por la Comisión.

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

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

([25]) 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).

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

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

7. El programa de trabajo plurianual fijará la programación estratégica general, incluidos los objetivos, los resultados esperados y los indicadores de rendimiento. Definirá asimismo la programación de los recursos, en particular el presupuesto plurianual y el personal.

8. La programación de los recursos se actualizará todos los años. La programación estratégica se actualizará cuando proceda, y en particular cuando resulte necesario a la luz de los resultados de la evaluación a que se refiere el artículo 67.

Artículo 25

Declaración de intereses

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

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

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

Artículo 26

Transparencia

1. ENISA llevará a cabo sus actividades con un alto grado de transparencia y de conformidad con el artículo 28.

2. ENISA velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo. Asimismo, deberá hacer públicas las declaraciones de intereses realizadas de conformidad con el artículo 25.

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

4. ENISA establecerá en sus normas internas de funcionamiento, las medidas prácticas de aplicación de las normas de transparencia a que se refieren los apartados 1 y 2.

Artículo 27

Confidencialidad

1. Sin perjuicio de lo dispuesto en el artículo 28, ENISA no divulgará a terceros la información que trate o reciba para la que se haya presentado una solicitud motivada de tratamiento confidencial.

2. Los miembros del Consejo de Administración, el director ejecutivo, los miembros del Grupo Consultivo de ENISA, los expertos externos que participen en los grupos de trabajo *ad hoc* y los miembros del personal de ENISA, incluidos los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal, respetarán la obligación de confidencialidad prevista en el artículo 339 del TFUE, incluso después de haber cesado en sus funciones.

3. ENISA establecerá en sus normas internas de funcionamiento las medidas prácticas de aplicación de las normas de confidencialidad a que se refieren los apartados 1 y 2.

4. Si así lo exige el desempeño de los cometidos de ENISA, el Consejo de Administración tomará la decisión de permitir a ENISA manejar información clasificada. En tal caso, ENISA, de común acuerdo con los servicios de la Comisión, adoptará unas normas de seguridad que aplique los principios de seguridad contenidos en las Decisiones (UE, Euratom) 2015/443 ([26]) y 2015/444 ([27]) de la Comisión. Dichas normas de seguridad incluirán, entre otras, disposiciones para el intercambio, tratamiento y almacenamiento de la información clasificada.

Artículo 28

Acceso a los documentos

1. El Reglamento (CE) n.º 1049/2001 se aplicará a los documentos en poder de ENISA.

2. El Consejo de Administración adoptará disposiciones para la aplicación del Reglamento (CE) n.º 1049/2001 a más tardar el 28 de diciembre de 2019.

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

CAPÍTULO IV

Establecimiento y estructura del presupuesto de ENISA

Artículo 29

Establecimiento del presupuesto de ENISA

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

2. El Consejo de Administración presentará cada año, sobre la base del proyecto de estado de previsiones un estado de previsiones de ingresos y gastos de ENISA para el siguiente ejercicio financiero.

3. El Consejo de Administración, a más tardar el 31 de enero de cada año, transmitirá el estado de previsiones, que formará parte del proyecto de documento único de programación, a la Comisión y a los terceros países con los que la Unión haya celebrado acuerdos de conformidad con el artículo 42, apartado 2.

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

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

6. El Parlamento Europeo y el Consejo adoptarán la plantilla de ENISA.

([26]) 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).

([27]) 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).

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

Artículo 30

Estructura del presupuesto de ENISA

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

a) una contribución procedente del presupuesto general de la Unión;

b) ingresos asignados a partidas de gastos específicas de conformidad con las normas financieras mencionadas en el artículo 32;

c) financiación de la Unión en forma de convenios de delegación o subvenciones *ad hoc*, de conformidad con las normas financieras mencionadas en el artículo 32 y las disposiciones de los instrumentos pertinentes de apoyo a las políticas de la Unión;

d) contribuciones de terceros países que participen en los trabajos de ENISA a que se refiere el artículo 42;

e) eventuales contribuciones voluntarias, dinerarias o en especie, de los Estados miembros.

Los Estados miembros que aporten contribuciones voluntarias en virtud del párrafo primero, letra e), no podrán reclamar ningún derecho o servicio específico como consecuencia de su contribución.

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

Artículo 31

Ejecución del presupuesto de ENISA

1. El director ejecutivo será responsable de la ejecución del presupuesto de ENISA.

2. El auditor interno de la Comisión ejercerá, con respecto a ENISA, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión.

3. El contable de ENISA remitirá las cuentas provisionales del ejercicio financiero (ejercicio N) al contable de la Comisión y al Tribunal de Cuentas a más tardar el 1 de marzo del ejercicio financiero siguiente (ejercicio N+1).

4. Tras recibir las observaciones formuladas por el Tribunal de Cuentas sobre las cuentas provisionales de ENISA, de conformidad con el artículo 246 del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo ([28]), el contable de ENISA elaborará las cuentas definitivas de ENISA bajo su responsabilidad y las presentará al Consejo de Administración para que este emita dictamen al respecto.

5. El Consejo de Administración emitirá un dictamen sobre las cuentas definitivas de ENISA.

6. A más tardar el 31 de marzo del año N + 1, el director ejecutivo remitirá el informe sobre la gestión presupuestaria y financiera al Parlamento Europeo, al Consejo, a la Comisión y al Tribunal de Cuentas.

7. A más tardar el 1 de julio del año N + 1, el contable de ENISA remitirá las cuentas definitivas de ENISA, juntamente con el dictamen del Consejo de Administración, al Parlamento Europeo, al Consejo, al contable de la Comisión y al Tribunal de Cuentas.

([28]) Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1).

8. En la misma fecha de transmisión de sus cuentas definitivas, el contable de ENISA también enviará al Tribunal de Cuentas una toma de posición relativa a estas cuentas definitivas, con copia al contable de la Comisión.

9. El director ejecutivo publicará las cuentas definitivas de ENISA en el *Diario Oficial de la Unión Europea* a más tardar el 15 de noviembre del año N + 1.

10. A más tardar el 30 de septiembre del año N + 1, el director ejecutivo remitirá al Tribunal de Cuentas una respuesta a sus observaciones, y enviará asimismo copia de dicha respuesta al Consejo de Administración y a la Comisión.

11. El director ejecutivo presentará al Parlamento Europeo, cuando este lo solicite, toda la información necesaria para el correcto desarrollo del procedimiento de aprobación de la ejecución del presupuesto del ejercicio de que se trate, de conformidad con el artículo 261, apartado 3, del Reglamento (UE, Euratom) 2018/1046.

12. El Parlamento Europeo, sobre la base de una recomendación del Consejo, deberá aprobar, antes del 15 de mayo del año N+ 2, la gestión del director ejecutivo respecto a la ejecución del presupuesto del año N.

Artículo 32

Normas financieras

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

Artículo 33

Lucha contra el fraude

1. Con el fin de facilitar la lucha contra el fraude, la corrupción y otras actividades ilegales con arreglo al Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo ([29]), ENISA, a más tardar el 28 de diciembre de 2019, suscribirá el Acuerdo Interinstitucional, de 25 de mayo de 1999, entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión de las Comunidades Europeas, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) ([30]), y adoptará las disposiciones apropiadas, que serán de aplicación a todo el personal de ENISA, sirviéndose del modelo contenido en el anexo de dicho Acuerdo.

2. El Tribunal de Cuentas tendrá la facultad de auditar, a partir de documentos e información obtenida a raíz de inspecciones *in situ*, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido de ENISA fondos de la Unión.

3. La OLAF podrá realizar investigaciones, incluidos controles y verificaciones sobre el terreno, de conformidad con las disposiciones y los procedimientos establecidos en el Reglamento n.º 883/2013 y el Reglamento (Euratom, CE) n.º 2185/96 ([31]) del Consejo, con el fin de determinar si ha habido fraude, corrupción o cualquier otra actividad ilegal que afecte a los intereses financieros de la Unión en relación con una subvención o un contrato financiado por ENISA.

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

([29]) 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).

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

([31]) 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).

CAPÍTULO V

Personal

Artículo 34

Disposiciones generales

El Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, así como las normas adoptadas de común acuerdo entre las instituciones de la Unión con el fin de poner en práctica el Estatuto de los funcionarios y el Régimen aplicable a los otros agentes, se aplicarán al personal de ENISA.

Artículo 35

Privilegios e inmunidades

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

Artículo 36

Director ejecutivo

1. El director ejecutivo será contratado como agente temporal de ENISA según lo dispuesto en el artículo 2, letra a), del Régimen aplicable a los otros agentes.

2. El director ejecutivo será nombrado por el Consejo de Administración a partir de una lista de candidatos propuesta por la Comisión en el marco de un procedimiento de selección abierto y transparente.

3. Para la celebración del contrato del director ejecutivo, ENISA estará representada por el presidente del Consejo de Administración.

4. Antes del nombramiento, se invitará al candidato seleccionado por el Consejo de Administración a hacer una declaración ante la comisión pertinente del Parlamento Europeo y a responder a las preguntas formuladas por los diputados.

5. El mandato del director ejecutivo tendrá una duración de cinco años. Al final de ese período, la Comisión realizará una evaluación de la actuación del director ejecutivo y de las futuras tareas y desafíos de ENISA.

6. El Consejo de Administración se pronunciará sobre el nombramiento, la prórroga del mandato o el cese del director ejecutivo de conformidad con el artículo 18, apartado 2.

7. A propuesta de la Comisión, en la que se tendrá en cuenta la evaluación a que se refiere el apartado 5, el Consejo de Administración podrá prorrogar una vez el mandato del director ejecutivo, por cinco años.

8. El Consejo de Administración informará al Parlamento Europeo acerca de su intención de prorrogar el mandato del director ejecutivo. En los tres meses que precedan a la prórroga de su mandato, el director ejecutivo hará, si se le invita a ello, una declaración ante la comisión pertinente del Parlamento Europeo y responderá a las preguntas formuladas por los parlamentarios.

9. Un director ejecutivo cuyo mandato haya sido prorrogado no podrá participar en otro procedimiento de selección para el mismo puesto.

10. El director ejecutivo solo podrá ser cesado por una decisión del Consejo de Administración, a propuesta de la Comisión.

Artículo 37

Expertos nacionales en comisión de servicios y otros agentes

1. ENISA podrá recurrir a expertos nacionales en comisión de servicios o a otro personal no contratado por ENISA. El Estatuto de los funcionarios y el Régimen aplicable a los otros agentes no serán de aplicación a este personal.

2. El Consejo de Administración adoptará una decisión que establezca las normas aplicables a las comisiones de servicios de expertos nacionales en ENISA.

CAPÍTULO VI

Disposiciones generales relativas a ENISA

Artículo 38

Estatuto jurídico de ENISA

1. ENISA será un órgano de la Unión dotado de personalidad jurídica.

2. En cada Estado miembro, ENISA disfrutará de la capacidad jurídica más amplia que se conceda a las personas jurídicas en el Derecho interno. En particular, podrá adquirir o vender propiedad mobiliaria e inmobiliaria y ser parte en actuaciones judiciales.

3. ENISA estará representada por su director ejecutivo.

Artículo 39

Responsabilidad de ENISA

1. La responsabilidad contractual de ENISA se regirá por la legislación aplicable al contrato de que se trate.

2. El Tribunal de Justicia de la Unión Europea será competente para pronunciarse en virtud de cualquier cláusula arbitral contenida en un contrato firmado por ENISA.

3. En materia de responsabilidad extracontractual, ENISA deberá reparar los daños causados por ella o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a las legislaciones de los Estados miembros.

4. El Tribunal de Justicia de la Unión Europea será competente para conocer de todos los litigios relativos a la indemnización por los daños a que se refiere el apartado 3.

5. La responsabilidad personal del personal de ENISA respecto a ENISA se regirá por las disposiciones pertinentes aplicables al personal de ENISA.

Artículo 40

Régimen lingüístico

1. El Reglamento n.º 1 del Consejo será aplicable a ENISA ([32]). Los Estados miembros y los demás organismos nombrados por los Estados miembros podrán dirigirse a ENISA y obtener respuesta en la lengua oficial de las instituciones de la Unión Europea que elijan.

2. Los servicios de traducción requeridos para el funcionamiento de ENISA serán prestados por el Centro de traducción de los órganos de la Unión Europea.

Artículo 41

Protección de los datos de carácter personal

1. El tratamiento de los datos de carácter personal por parte de ENISA deberá ajustarse al Reglamento (UE) 2018/1725.

2. El Consejo de Administración adoptará las normas de ejecución a que se refiere el artículo 45, apartado 3, del Reglamento (UE) 2018/1725. El Consejo de Administración podrá adoptar otras medidas suplementarias necesarias para la aplicación del Reglamento (UE) 2018/1725 por parte de ENISA.

([32]) Reglamento n.º 1 por el que se fija el régimen lingüístico de la Comunidad Económica Europea (DO 17 de 6.10.1958, p. 385).

Artículo 42

Cooperación con terceros países y organizaciones internacionales

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

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

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

Artículo 43

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

Previa consulta a la Comisión, ENISA adoptará sus normas de seguridad aplicando los principios de seguridad contenidos en las normas de seguridad de la Comisión para la protección de la información sensible no clasificada y la ICUE, según lo dispuesto en las Decisiones (UE, Euratom) 2015/443 y 2015/444. Las normas de seguridad de ENISA incluirán disposiciones para el intercambio, tratamiento y almacenamiento de este tipo de información.

Artículo 44

Acuerdo relativo a la sede y condiciones de funcionamiento

1. Las disposiciones necesarias relativas al alojamiento que debe proporcionarse a ENISA en el Estado miembro de acogida y las instalaciones que debe poner a disposición dicho Estado miembro, así como las normas específicas aplicables en el Estado miembro de acogida al Director Ejecutivo, los miembros del Consejo de Administración, el personal de ENISA y los miembros de sus familias se establecerán en un acuerdo de sede entre ENISA y el Estado miembro donde se encuentre la sede, celebrado previa aprobación del Consejo de Administración.

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

Artículo 45

Control administrativo

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

TÍTULO III

MARCO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD

Artículo 46

Marco europeo de certificación de la ciberseguridad

1. Se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC.

2. El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida.

Artículo 47

Programa de trabajo evolutivo de la Unión para la certificación europea de la ciberseguridad

1. La Comisión publicará un programa de trabajo evolutivo para los esquemas europeos de certificación de la ciberseguridad (en lo sucesivo, «programa de trabajo evolutivo de la Unión») que definirá las prioridades estratégicas para los futuros esquemas europeos de certificación de la ciberseguridad.

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

3. Se justificará la inclusión de un producto, servicio o proceso de TIC específico, o de categorías de los mismos, en un programa de trabajo evolutivo de la Unión, sobre la base de uno o más de los siguientes motivos:

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

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

c) la demanda del mercado;

d) la evolución del panorama de las ciberamenazas;

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

4. La Comisión tendrá debidamente en cuenta los dictámenes emitidos por el GECC y por el Grupo de las Partes Interesadas sobre Certificación del proyecto de programa de trabajo evolutivo de la Unión.

5. El primer programa de trabajo evolutivo de la Unión se publicará a más tardar el 10 de junio de 2020. El programa de trabajo evolutivo de la Unión se actualizará una vez cada tres años y más a menudo en caso necesario.

Artículo 48

Solicitud de un esquema europeo de certificación de la ciberseguridad

1. La Comisión podrá solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad existente basándose en el programa de trabajo evolutivo de la Unión.

2. En casos debidamente justificados, la Comisión o el GECC podrán solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad existente que no esté incluido en el programa de trabajo evolutivo de la Unión. El programa de trabajo evolutivo de la Unión se actualizará en consecuencia.

Artículo 49

Preparación, adopción y revisión de esquemas europeos de certificación de la ciberseguridad

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

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

3. A la hora de preparar las propuestas de esquema ENISA consultará a todas las partes interesadas mediante un proceso de consulta oficial transparente e inclusivo.

4. Para cada propuesta de esquema, ENISA creará un grupo *ad hoc* con arreglo al artículo 20, apartado 4, con el objetivo de facilitar a ENISA asesoramiento y conocimientos específicos.

5. ENISA cooperará estrechamente con el GECC. El GECC facilitará a ENISA la asistencia y el asesoramiento experto en relación con la preparación de la propuesta de esquema y adoptará un dictamen sobre la propuesta de esquema.

6. ENISA tomará en máxima consideración el dictamen del GECC antes de transmitir a la Comisión la propuesta de esquema preparada de conformidad con los apartados 3, 4 y 5. El dictamen del GECC no es vinculante para ENISA y su ausencia no impedirá a ENISA transmitir la propuesta de esquema a la Comisión.

7. La Comisión, a partir de la propuesta de esquema preparada por ENISA, podrá adoptar actos de ejecución que establezcan esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC que cumplan los requisitos de los artículos 51, 52 y 54. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 66, apartado 2.

8. ENISA evaluará al menos cada cinco años los esquemas europeos de certificación de la ciberseguridad teniendo en cuenta los comentarios recibidos de las partes interesadas. Si lo considera necesario, la Comisión o el GECC podrán pedir a ENISA que dé inicio al proceso de elaboración de una propuesta revisada de esquema conforme al artículo 48 y al presente artículo.

Artículo 50

Sitio web **de los esquemas europeos de certificación de la ciberseguridad**

1. ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los esquemas europeos de certificación de la ciberseguridad, los certificados europeos de la ciberseguridad y las declaraciones UE de conformidad y darles publicidad, también en lo que se refiere a los esquemas europeos de certificación de la ciberseguridad que ya no son válidos y certificados europeos de la ciberseguridad y las declaraciones UE de conformidad retirados o caducados y al repositorio de hiperenlaces de información sobre ciberseguridad facilitado de conformidad con el artículo 55.

2. En su caso, el sitio web al que se refiere el apartado 1 indicará asimismo aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

Artículo 51

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

Los esquemas europeos de certificación de la ciberseguridad deberán diseñarse para cumplir, según proceda, al menos los siguientes objetivos de seguridad:

a) proteger los datos almacenados, transmitidos o tratados de otro modo frente al almacenamiento, tratamiento, acceso o revelación accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso de TIC;

b) proteger los datos almacenados, transmitidos o tratados de otro modo frente a la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso de TIC;

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

d) detectar y documentar las dependencias y vulnerabilidades conocidas;

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

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

g) verificar que los productos, servicios y procesos de TIC no contengan vulnerabilidades conocidas;

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

i) que los productos, servicios y procesos de TIC sean seguros por defecto y desde el diseño;

j) que los productos, servicios y procesos de TIC se entreguen siempre con un programa informático y un equipo informático actualizados que no contengan vulnerabilidades conocidas públicamente, y dispongan de mecanismos para efectuar actualizaciones de seguridad.

Artículo 52

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

1. Un esquema europeo de certificación de la ciberseguridad podrá especificar uno o más de los niveles de garantía siguientes para los productos, servicios y procesos de TIC: «básico», «sustancial» o «elevado». El nivel de garantía deberá reflejar el nivel de riesgo asociado al uso previsto de un producto, servicio o proceso de TIC, en términos de probabilidad y repercusiones de un incidente.

2. Los certificados europeos de ciberseguridad o las declaraciones de conformidad de la UE mencionarán el nivel de garantía especificado en el esquema europeo de certificación de la ciberseguridad en el marco del cual ha sido expedido el certificado europeo de ciberseguridad o la declaración de conformidad de la UE.

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

4. El certificado o la declaración de la conformidad de la UE hará referencia a especificaciones técnicas, normas y procedimientos conexos, incluidos los controles técnicos, cuyo objetivo es reducir el riesgo de incidentes de ciberseguridad o evitarlos.

5. Un certificado europeo de ciberseguridad o una declaración de la conformidad de la UE que se refiere a un nivel de garantía «básico» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado o esa declaración de la conformidad cumplen los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos básicos conocidos de ciberincidentes y ciberataques. Las actividades de evaluación a efectuar incluirán al menos una revisión de la documentación técnica. Cuando dicha revisión no sea apropiada, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

6. Un certificado europeo de ciberseguridad que se refiere a un nivel de garantía «sustancial» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado cumplen los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos relacionados con la ciberseguridad conocidos, los riesgos de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados. Las actividades de evaluación a efectuar incluirán al menos: la revisión para demostrar la ausencia de las vulnerabilidades conocidas públicamente y la comprobación de que los productos, servicios o procesos de TIC aplican correctamente las funcionalidades de seguridad necesarias. Cuando dichas actividades de evaluación no sean apropiadas, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

7. Un certificado europeo de ciberseguridad que se refiere a un nivel de garantía «elevado» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado cumplen los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables.

Las actividades de evaluación a efectuar incluirán al menos: la revisión de la improcedencia de las vulnerabilidades conocidas públicamente, la comprobación de que los productos, procesos o servicios de TIC aplican correctamente la necesaria funcionalidad de seguridad, con las tecnologías más avanzadas, y la evaluación de su resistencia a atacantes expertos mediante pruebas de penetración. Cuando dichas actividades no sean apropiadas, se emprenderán actividades de evaluación de la sustitución con efecto equivalente.

8. Un esquema europeo de certificación de la ciberseguridad podrá especificar varios niveles de evaluación en función del rigor y la profundidad de los métodos de evaluación. Cada uno de los niveles de evaluación corresponderá a uno de los niveles de garantía y estará definido por una combinación apropiada de componentes de garantía.

Artículo 53

Autoevaluación de la conformidad

1. Un esquema europeo de certificación de la ciberseguridad podrá permitir realizar una autoevaluación de la conformidad bajo la responsabilidad exclusiva del fabricante o proveedor de productos, servicios o procesos de TIC. La autoevaluación de la conformidad únicamente se permitirá en relación con productos, servicios y procesos de TIC que presenten un bajo riesgo correspondientes al nivel de garantía «básico».

2. El fabricante o el proveedor de los productos, servicios o procesos de TIC puede expedir una declaración de conformidad de la UE donde declare que queda demostrado el cumplimiento de los requisitos establecidos por el esquema. Al establecer dicha declaración, el fabricante o proveedor de productos, servicios o procesos de TIC asumirá la responsabilidad de la conformidad del producto, servicio o proceso de TIC con los requisitos que establezca dicho esquema.

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

4. La expedición de una declaración de conformidad de la UE será voluntaria, a menos que el Derecho de la Unión o de los Estados miembros especifique lo contrario.

5. Las declaraciones de conformidad de la UE serán reconocidas en todos los Estados miembros.

Artículo 54

Elementos de los esquemas europeos de certificación de la ciberseguridad

1. Un esquema europeo de certificación de la ciberseguridad incluirá al menos los siguientes elementos:

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

b) una descripción clara de la finalidad del esquema y de la manera en que las normas, los métodos de evaluación y los niveles de garantía seleccionados corresponden a las necesidades de los usuarios previstos del esquema;

c) referencias a las normas internacionales, europeas o nacionales que se han seguido para hacer la evaluación. En caso de que no haya normas disponibles, o de que estas no sean adecuadas, se deberá hacer referencia a las especificaciones técnicas que cumplen los requisitos del anexo II del Reglamento (UE) n.º 1025/2012 o, si no estuvieran disponibles, a las especificaciones técnicas o a otros requisitos de ciberseguridad definidos en el esquema europeo de certificación de la ciberseguridad;

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

e) una indicación de si está permitida, en virtud del esquema, la autoevaluación de la conformidad;

f) en su caso, requisitos específicos o adicionales a los que están sujetos los organismos de evaluación de la conformidad a fin de garantizar su capacidad técnica para evaluar los requisitos en materia de ciberseguridad;

g) los criterios y métodos de evaluación específicos que deben ser utilizados, incluidos los tipos de evaluación, para demostrar el logro de los objetivos de seguridad a que se refiere el artículo 51;

h) en su caso, la información necesaria para la certificación que un solicitante debe facilitar a los organismos de evaluación de la conformidad o poner a su disposición de otro modo;

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

j) las normas para controlar el cumplimiento de los productos, servicios y procesos de TIC de los requisitos de los certificados europeos de ciberseguridad o de la declaración de conformidad de la UE, incluidos los mecanismos que permitan demostrar la conformidad permanente con los requisitos de ciberseguridad especificados;

k) en su caso, condiciones para la expedición, el mantenimiento, la continuación y la renovación de un certificado europeo de ciberseguridad, así como condiciones para la ampliación o la reducción del alcance de la certificación;

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

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

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

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

p el contenido y formato de los certificados europeos de ciberseguridad y de la declaración de conformidad de la UE que van a ser expedidos;

q) el período de disponibilidad de la declaración de conformidad de la UE, la documentación técnica y toda otra información pertinente proporcionada por el fabricante o el proveedor de productos, servicios o procesos de TIC;

r) el período máximo de validez de los certificados europeos de ciberseguridad expedidos en virtud del esquema;

s) la política de divulgación para los certificados europeos de ciberseguridad expedidos, modificados o retirados en virtud del esquema;

t) las condiciones para el reconocimiento mutuo de los esquemas de certificación con terceros países;

u) en su caso, normas relativas a cualquier mecanismo de evaluación interpares establecido en el esquema respecto de las autoridades u organismos que expidan certificados europeos de ciberseguridad para niveles de garantía «elevados» con arreglo al artículo 56, apartado 6. Dicho mecanismo se entenderá sin perjuicio de las revisiones interpares previstas en el artículo 59;

v) formato y procedimientos que deben seguir los fabricantes y proveedores de productos, servicios o procesos de TIC para proporcionar y actualizar la información complementaria sobre ciberseguridad de conformidad con el artículo 55.

2. Los requisitos específicos del esquema europeo de certificación de la ciberseguridad serán coherentes con los requisitos legales aplicables, en particular los requisitos que emanen de las disposiciones armonizadas del Derecho de la Unión.

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

4. En ausencia de disposiciones armonizadas del Derecho de la Unión, el Derecho de un Estado miembro podrá prever también el uso de un esquema europeo de certificación de la ciberseguridad para establecer la presunción de conformidad con los requisitos legales.

Artículo 55

Información complementaria sobre ciberseguridad de productos, servicios y procesos de TIC certificados

1. El fabricante o proveedor de productos, servicios y procesos de TIC certificados o autoevaluados proporcionará la información sobre ciberseguridad complementaria siguiente:

a) orientaciones y recomendaciones para ayudar a los usuarios finales con la configuración, la instalación, el despliegue, el funcionamiento y el mantenimiento seguros de los productos o servicios de TIC;

b) el período durante el cual se ofrecerá a los usuarios finales apoyo en materia de seguridad, en particular en lo que se refiere a la disponibilidad de actualizaciones relacionadas con la ciberseguridad;

c) datos de contacto del fabricante o proveedor y métodos aceptados para recibir información sobre vulnerabilidad de usuarios finales o investigadores en materia de seguridad;

d) una referencia a los registros en línea en los que consten las vulnerabilidades conocidas públicamente en relación con el producto, servicio o proceso de TIC, así como recomendaciones pertinentes en materia de ciberseguridad.

2. La información a que se refiere el apartado 1 estará disponible en formato electrónico y seguirá estando disponible y siendo actualizada en función de las necesidades al menos hasta la expiración del correspondiente certificado europeo de ciberseguridad o de la declaración de conformidad de la UE.

Artículo 56

Certificación de la ciberseguridad

1. Los productos, servicios y procesos de TIC que hayan sido certificados de conformidad con un esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 49 se presumirán conformes con los requisitos de dicho esquema.

2. La certificación de la ciberseguridad será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros.

3. La Comisión evaluará periódicamente la eficacia y la utilización de los esquemas europeos de certificación de la ciberseguridad adoptados, así como si un esquema europeo de certificación de la ciberseguridad específico debe convertirse en obligatorio mediante el Derecho de la Unión aplicable para garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión y mejorar el funcionamiento del mercado interior. La primera de tales evaluaciones debe efectuarse a más tardar el 31 de diciembre de 2023, y las evaluaciones posteriores como mínimo cada dos años. La Comisión deberá, con base en los resultados de la evaluación, determinar los productos, servicios y procesos de TIC cubiertos por un esquema de certificación existente que deben estar cubiertos por un esquema de certificación obligatorio.

La Comisión atenderá, con carácter prioritario, a los sectores enumerados en el anexo II de la Directiva (UE) 2016/1148, que se evaluarán a más tardar dos años después de la adopción del primer esquema europeo de certificación de la ciberseguridad.

Al preparar la evaluación, la Comisión deberá:

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

b) tener en cuenta la existencia y la aplicación del Derecho del Estado miembro y del tercer país pertinentes;

c) llevar a cabo un procedimiento de consulta abierto, transparente e inclusivo con todas las partes interesadas pertinentes y los Estados miembros;

d) tener en cuenta los plazos de aplicación, los períodos y medidas transitorios, en particular, respecto de las posibles repercusiones de la medida sobre los fabricantes o los proveedores de productos, servicios y procesos de TIC, incluidas las pymes;

e) proponer la manera más rápida y eficaz para llevar a cabo la transición entre un esquema de certificación voluntario y uno obligatorio.

4. Los organismos de evaluación de la conformidad a que se refiere el artículo 60 expedirán un certificado europeo de ciberseguridad en virtud del presente artículo que haga referencia al nivel de garantía «básico» o «sustancial», sobre la base de los criterios incluidos en el esquema europeo de certificación de la ciberseguridad adoptado por la Comisión de conformidad con el artículo 49.

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

a) una autoridad nacional de certificación de la ciberseguridad con arreglo al artículo 58, apartado 1, o

b) un organismo público que esté acreditado como organismo de evaluación de la conformidad con arreglo al artículo 60, apartado 1.

6. En los casos en que un esquema europeo de certificación de la ciberseguridad adoptado en virtud del artículo 49 requiera un nivel de garantía «elevado», el certificado europeo de ciberseguridad en virtud de dicho esquema solo podrá ser expedido por una autoridad nacional de certificación de la ciberseguridad o, en los siguientes casos, por un organismo de evaluación de la conformidad:

a) previa aprobación de la autoridad nacional de certificación de la ciberseguridad para cada certificado europeo de ciberseguridad individual que expida un organismo de evaluación de la conformidad, o

b) con base en una delegación general de la tarea de expedir tal certificado europeo de ciberseguridad por la autoridad nacional de certificación de la ciberseguridad a un organismo de evaluación de la conformidad.

7. La persona física o jurídica que presenta los productos, servicios o procesos de TIC para la certificación pondrá a disposición de la autoridad nacional de certificación de la ciberseguridad a que se refiere el artículo 58, si dicha autoridad es el organismo que expide el certificado europeo de ciberseguridad, o del organismo de evaluación de la conformidad a que se refiere el artículo 60, toda la información necesaria para llevar a cabo el procedimiento de certificación.

8. El titular de un certificado europeo de ciberseguridad informará a la autoridad o al organismo a que se refiere el apartado 7, de cualquier vulnerabilidad o irregularidad que se detecte posteriormente, relativa a la seguridad del producto, servicio o proceso de TIC certificado, que pueda afectar al cumplimiento de los requisitos de certificación. La citada autoridad u organismo transmitirán dicha información sin demora indebida a la autoridad nacional de certificación de la ciberseguridad de que se trate.

9. Los certificados europeos de ciberseguridad se expedirán por el período previsto en el esquema europeo de certificación de la ciberseguridad y podrán renovarse siempre y cuando sigan cumpliéndose los requisitos correspondientes.

10. Los certificados europeos de ciberseguridad expedidos en virtud del presente artículo serán reconocidos en todos los Estados miembros.

Artículo 57

Esquemas y certificados nacionales de certificación de la ciberseguridad

1. Sin perjuicio de lo dispuesto en el apartado 3 del presente artículo, los esquemas nacionales de certificación de ciberseguridad y los procedimientos correspondientes para los productos, servicios y procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad dejarán de surtir efectos a partir de la fecha establecida en el acto de ejecución adoptado con arreglo al artículo 49, apartado 7. Los esquemas nacionales de certificación de la ciberseguridad y los procedimientos conexos para los productos, servicios y procesos de TIC que no estén cubiertos por un esquema europeo de certificación de la ciberseguridad seguirán existiendo.

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

3. Los certificados existentes expedidos de conformidad con esquemas nacionales de certificación de la ciberseguridad y cubiertos por un esquema europeo de certificación de la ciberseguridad seguirán siendo válidos hasta su fecha de caducidad.

4. Con vistas a evitar la fragmentación del mercado interior, los Estados miembros informarán a la Comisión y al GECC cualquier intención de crear nuevos esquemas nacionales de certificación de la ciberseguridad.

Artículo 58

Autoridades nacionales de certificación de la ciberseguridad

1. Cada Estado miembro designará a una o más autoridades nacionales de certificación de la ciberseguridad en su territorio o, de mutuo acuerdo con otro Estado miembro, designará a una o más autoridades nacionales de certificación de la ciberseguridad establecidas en ese otro Estado miembro para que se encarguen de las tareas de supervisión en el Estado miembro que efectúe la designación.

2. Cada Estado miembro informará a la Comisión de la identidad de las autoridades nacionales de certificación de la ciberseguridad designadas. Cuando un Estado miembro designe más de una autoridad, también informará a la Comisión de las tareas que se hayan encomendado a cada una de dichas autoridades.

3. Sin perjuicio de lo establecido en el artículo 56, apartado 5), y en el artículo 56, apartado 6, las autoridades nacionales de certificación de la ciberseguridad serán, en lo relativo a su organización, sus decisiones de financiación, su estructura jurídica y su proceso de toma de decisiones, independientes de las entidades que están bajo su supervisión.

4. Los Estados miembros se asegurarán de que las actividades de las autoridades nacionales de certificación de la ciberseguridad relacionadas con la expedición de certificados europeos de ciberseguridad de conformidad con el artículo 56, apartado 5, letra a), y el artículo 56, apartado 6, están estrictamente separadas de las actividades de supervisión establecidas en el presente artículo y de que dichas actividades se desempeñan de manera independiente una de la otra.

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

6. Para la aplicación eficaz del presente Reglamento, es conveniente que estas autoridades nacionales de certificación de la ciberseguridad participen en el GECC manera activa, eficaz, eficiente y segura.

7. Las autoridades nacionales de certificación de la ciberseguridad:

a) supervisarán y velarán por la aplicación de las normas recogidas en los esquemas europeos de certificación de la ciberseguridad en virtud del artículo 54, apartado 1, letra j), para controlar la conformidad de los productos, servicios y procesos de TIC con los requisitos de los certificados europeos de la ciberseguridad que hayan sido expedidos en sus respectivos territorios, en cooperación con otras autoridades de vigilancia del mercado pertinentes;

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

c) sin perjuicio de lo dispuesto en el artículo 60, apartado 3, asistirán y apoyarán activamente a los organismos nacionales de acreditación en el control y la supervisión de las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento;

d) controlarán y supervisarán las actividades de los organismos públicos mencionados en el artículo 56, apartado 5;

e) cuando proceda, autorizarán a los organismos de evaluación de la conformidad con arreglo al artículo 60, apartado 3, y restringirán, suspenderán o retirarán las autorizaciones en vigor en caso de incumplimiento, por parte de los organismos de evaluación de la conformidad, de los requisitos del presente Reglamento;

f) tramitarán las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados europeos de ciberseguridad expedidos por las autoridades nacionales de certificación de la ciberseguridad o los certificados europeos de ciberseguridad expedidos por los organismos de evaluación de la conformidad, de conformidad con el artículo 56, apartado 6, o en relación con las declaraciones de conformidad UE expedidas en virtud del artículo 53, investigarán el asunto objeto de la reclamación en la medida que proceda e informarán al reclamante sobre el curso y el resultado de la investigación en un plazo razonable;

g) presentarán a ENISA y al GECC un informe sucinto anual de las actividades realizadas con arreglo a las letras b), c) y d) del presente apartado y al apartado 8;

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

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

8. Cada autoridad nacional de certificación de la ciberseguridad tendrá, como mínimo, las siguientes competencias:

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

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

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

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

e) retirar, con arreglo al Derecho nacional, los certificados europeos de ciberseguridad expedidos por la autoridad nacional de certificación de la ciberseguridad o los certificados europeos de ciberseguridad expedidos por los organismos de evaluación de la conformidad, de conformidad con el artículo 56, apartado 6, que no se ajusten al presente Reglamento o a un esquema europeo de certificación de la ciberseguridad;

f) imponer sanciones conforme al Derecho nacional según lo establecido en el artículo 65, y solicitar el cese inmediato de la violación de las obligaciones establecidas en el presente Reglamento.

9. Las autoridades nacionales de certificación de la ciberseguridad cooperarán entre ellas y con la Comisión y, en particular, intercambiarán información, experiencias y buenas prácticas en relación con la certificación de la ciberseguridad y las cuestiones técnicas relativas a la ciberseguridad de los productos, servicios y procesos de TIC.

Artículo 59

Revisión interpares

1. Con vistas a alcanzar normas equivalentes en toda la Unión en lo que respecta a los certificados europeos de ciberseguridad expedidos y a las declaraciones de conformidad de la UE, las autoridades nacionales de certificación de la ciberseguridad serán objeto de revisiones interpares.

2. La revisión interpares se llevará a cabo conforme a criterios y procedimientos de evaluación bien fundados y transparentes, en particular en lo relativo a los requisitos estructurales, de recursos humanos y de proceso, la confidencialidad y las reclamaciones.

3. La revisión interpares deberá evaluar:

a) cuando corresponda, si las actividades de la autoridad nacional de certificación de la ciberseguridad relacionadas con la expedición de certificados europeos de ciberseguridad a que se refiere el artículo 56, apartado 5, letra a), y el artículo 56, apartado 6, se acogen a una estricta separación de funciones y responsabilidades con respecto a las actividades de supervisión de conformidad con el artículo 58 y si ambas actividades funcionan de manera independiente;

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

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

d) los procedimientos de control, autorización y supervisión de las actividades de los organismos de evaluación de la conformidad;

e) cuando corresponda, si el personal de las autoridades u organismos que expiden certificados para un nivel de garantía «elevado» en virtud del artículo 56, apartado 6, tiene los conocimientos técnicos apropiados.

4. La revisión interpares será realizada, como mínimo cada cinco años, por al menos dos autoridades nacionales de certificación de la ciberseguridad de otros Estados miembros y por la Comisión. ENISA podrá participar en la revisión interpares.

5. La Comisión estará facultada para adoptar actos de ejecución mediante el establecimiento de un plan para las revisiones interpares que cubra un período de al menos cinco años y mediante la definición de los criterios relativos a la composición del equipo de revisión interpares, la metodología utilizada para la revisión, así como el calendario, la periodicidad y las demás tareas relativas a dicha revisión. A la hora de adoptar esos actos de ejecución, la Comisión tendrá debidamente en cuenta las observaciones del GECC.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 66, apartado 2.

6. El GECC analizará los resultados de la revisión interpares y redactará un resumen que se podrá hacer público y que formulará, cuando sea necesario, orientaciones o recomendaciones sobre las acciones o medidas que deban tomar las entidades afectadas.

Artículo 60

Organismos de evaluación de la conformidad

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

2. Cuando una autoridad nacional de certificación de la ciberseguridad expida un certificado europeo de ciberseguridad de conformidad con el artículo 56, apartado 5, letra a), y el artículo 56 apartado 6, el organismo de certificación de la autoridad nacional de certificación de la ciberseguridad será acreditado como organismo de evaluación de la conformidad con arreglo al apartado 1 del presente artículo.

3. Cuando los esquemas europeos de certificación de la ciberseguridad establezcan requisitos específicos o adicionales con arreglo al artículo 54, apartado 1, letra f), únicamente los organismos de evaluación de la conformidad a los que la autoridad nacional de certificación de la ciberseguridad haya autorizado por cumplir dichos requisitos podrán realizar tareas en el marco de dichos esquemas.

4. La acreditación mencionada en el apartado 1 se expedirá a los organismos de evaluación de la conformidad por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de evaluación de la conformidad cumpla los requisitos establecidos en el presente artículo. Los organismos nacionales de acreditación tomarán todas las medidas necesarias dentro de un período razonable de tiempo para restringir, suspender o revocar la acreditación de un organismo de evaluación de la conformidad expedida en virtud del apartado 1 cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse, o si la actuación de dicho organismo de evaluación de la conformidad viola el presente Reglamento.

Artículo 61

Notificación

1. En relación con cada esquema europeo de certificación de la ciberseguridad adoptado, las autoridades nacionales de certificación de la ciberseguridad notificarán a la Comisión los correspondientes organismos de evaluación de la conformidad acreditados y, en su caso, autorizados de conformidad con el artículo 60, apartado 3, para expedir certificados europeos de ciberseguridad de los niveles de garantía especificados en el artículo 52. Las autoridades nacionales de certificación de la ciberseguridad notificarán, sin dilaciones indebidas, cualquier modificación al respecto.

2. Un año después de la entrada en vigor de un esquema europeo de certificación de la ciberseguridad, la Comisión publicará en el *Diario Oficial de la Unión Europea* una lista de los organismos de evaluación de la conformidad notificados en virtud del citado esquema.

3. Si la Comisión recibe una notificación una vez concluido el período a que se refiere el apartado 2, publicará en el *Diario Oficial de la Unión Europea* las modificaciones de la lista a que se refiere el apartado 2 en el plazo de dos meses a partir de la fecha de recepción de dicha notificación.

4. Una autoridad nacional de certificación de la ciberseguridad podrá presentar a la Comisión una solicitud para retirar de la lista a que se refiere el apartado 2 a un organismo de evaluación de la conformidad notificado por dicha autoridad. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de dicha lista en el plazo de un mes a partir de la fecha de recepción de la solicitud de la autoridad nacional de certificación de la ciberseguridad.

5. La Comisión podrá adoptar actos de ejecución para establecer las circunstancias, formatos y procedimientos de las notificaciones a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 66, apartado 2.

Artículo 62

Grupo Europeo de Certificación de la Ciberseguridad

1. Queda establecido el Grupo Europeo de Certificación de la Ciberseguridad (en lo sucesivo, «GECC»).

2. El GECC estará integrado por representantes de las autoridades nacionales de certificación de la ciberseguridad o por representantes de otras autoridades nacionales pertinentes. Cualquier miembro del GECC tan solo podrá representar a otro Estado miembro.

3. Las partes interesadas y terceras partes podrán ser invitadas a asistir a las reuniones del GECC y a participar en sus trabajos.

4. El GECC desempeñará las siguientes tareas:

a) asesorar y asistir a la Comisión en su labor de garantizar la coherencia en la implantación y aplicación del presente título, en particular en relación con el programa de trabajo evolutivo de la Unión, las cuestiones de política de certificación de la ciberseguridad, la coordinación de los enfoques políticos y la preparación de los esquemas europeos de certificación de la ciberseguridad;

b) asistir, asesorar y cooperar con ENISA en relación con la preparación de una propuesta de esquema, de conformidad con el artículo 49;

c) adoptar un dictamen sobre la propuesta de esquema preparada por ENISA, de conformidad con el artículo 49;

d) solicitar a ENISA que prepare una propuesta de esquema de conformidad con el artículo 48, apartado 2;

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

f) examinar las novedades pertinentes en el ámbito de la certificación de la ciberseguridad e intercambiar información y buenas prácticas sobre los esquemas de certificación de la ciberseguridad;

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

h) proporcionar apoyo a la aplicación de los mecanismos de evaluación interpares según las normas establecidas en un esquema europeo de certificación de la ciberseguridad de conformidad con el artículo 54, apartado 1, letra u);

i) facilitar el alineamiento de los esquemas europeos de certificación de la ciberseguridad con las normas internacionales reconocidas, en particular mediante la revisión de los esquemas europeos de certificación de la ciberseguridad existentes y, cuando proceda, mediante la formulación de recomendaciones a ENISA para que colabore con las organizaciones internacionales de normalización correspondientes al objeto de solucionar las deficiencias o lagunas en las normas vigentes reconocidas a nivel internacional.

5. Con la asistencia de ENISA, la Comisión presidirá el GECC y se hará cargo de su secretaría, de conformidad con el artículo 8, apartado 1, letra e).

Artículo 63

Derecho a presentar una reclamación

1. Las personas físicas o jurídicas tendrán derecho a presentar una reclamación ante el responsable de expedir un certificado europeo de ciberseguridad o, cuando la reclamación esté relacionada con un certificado europeo de ciberseguridad expedido por un organismo de evaluación de la conformidad que actúe con arreglo al artículo 56, apartado 6, ante la autoridad nacional de certificación de la ciberseguridad pertinente.

2. La autoridad u organismo ante el que se haya presentado la reclamación informará al reclamante sobre el curso del procedimiento y la decisión tomada, e informará al reclamante sobre el derecho de recurso a la tutela judicial efectiva a que se refiere el artículo 64.

Artículo 64

Derecho a la tutela judicial efectiva

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva en lo que respecta a:

a) las decisiones de la autoridad u organismo mencionado en el artículo 63, apartado 1, en particular y cuando corresponda en lo que respecta a la expedición, la no expedición o el reconocimiento de un certificado europeo de ciberseguridad del que sea titular dicha persona física o jurídica;

b) la inacción con respecto a una reclamación presentada ante la autoridad u organismo mencionado en el artículo 63, apartado 1.

2. Los recursos presentados en aplicación del presente artículo se dirimirán en los tribunales del Estado miembro donde se encuentre la autoridad u organismo ante el cual se plantea el procedimiento judicial.

Artículo 65

Sanciones

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

TÍTULO IV

DISPOSICIONES FINALES

Artículo 66

Procedimiento de comité

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

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5, apartado 4, letra b), del Reglamento (UE) n.º 182/2011.

Artículo 67

Evaluación y revisión

1. A más tardar el 28 de junio de 2024, y posteriormente cada cinco años, la Comisión evaluará el impacto, la eficacia y la eficiencia de ENISA y de sus prácticas de trabajo, así como la posible necesidad de modificar su mandato y las repercusiones financieras que tendría la eventual modificación. La evaluación tomará en consideración los comentarios llegados a ENISA en respuesta a sus actividades. Si la Comisión considerara que el funcionamiento continuado de ENISA ha dejado de estar justificada con respecto a los objetivos, mandato y tareas que le fueron atribuidos, la Comisión podrá proponer que se modifique el presente Reglamento en lo que se refiere a las disposiciones relacionadas con ENISA.

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

3. La evaluación valorará si son necesarios requisitos esenciales de ciberseguridad para el acceso al mercado interior a fin de evitar que se introduzcan en el mercado de la Unión productos, servicios y procesos de TIC que no cumplan los requisitos de base en materia de ciberseguridad.

4. A más tardar el 28 de junio de 2024, y posteriormente cada cinco años, la Comisión remitirá el informe de evaluación, conjuntamente con sus conclusiones, al Parlamento Europeo, al Consejo y al Consejo de Administración. Los resultados de dicho informe se harán públicos.

Artículo 68

Derogación y sucesión

1. Queda derogado el Reglamento (UE) n.º 526/2013, con efecto a partir del 27 de junio de 2019.

2. Las referencias al Reglamento (UE) n.º 526/2013 y a ENISA tal y como se establece por dicho Reglamento se entenderán hechas al presente Reglamento y a ENISA tal y como se establece por el presente Reglamento.

3. ENISA tal y como se establece por el presente Reglamento sucederá a la ENISA establecida por el Reglamento (UE) n.º 526/2013 en todo lo que se refiere a propiedad, acuerdos, obligaciones legales, contratos de empleo, compromisos financieros y responsabilidades. Todas las decisiones del Consejo de Administración y del Comité Ejecutivo adoptadas de conformidad con el Reglamento (UE) n. °526/2013 seguirán siendo válidas, a condición de que cumplen con lo dispuesto en el presente Reglamento.

4. ENISA se establecerá por un período indefinido a partir del 27 de junio de 2019.

5. El director ejecutivo nombrado de conformidad con el artículo 24, apartado 4, del Reglamento (UE) n.º 526/2013 permanecerá en el cargo y ejercerá las funciones del director ejecutivo a que se refiere el artículo 20 del presente Reglamento para el resto del mandato del director ejecutivo. Las demás condiciones de su contrato se mantendrán inalteradas

6. Los miembros del Consejo de Administración y sus suplentes designados de conformidad con el artículo 6 del Reglamento (UE) n.º 526/2013 permanecerán en el cargo y ejercerán las funciones del Consejo de Administración a que se refiere el artículo 15 del presente Reglamento para el resto de su mandato.

Artículo 69

Entrada en vigor

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

2. Los artículos 58, 60, 61, 63, 64 y 65, se aplicarán a partir del 28 de junio de 2021.

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

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

ANEXO

REQUISITOS QUE DEBEN CUMPLIR LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD

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

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

2. El organismo de evaluación de la conformidad será un organismo tercero independiente de la organización o de los productos, servicios o procesos de TIC 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, servicios o procesos 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, servicio o proceso de TIC que debe evaluarse, o el representante autorizado de ninguno de ellos. Dicha prohibición no será óbice para que se utilicen los productos de TIC evaluados necesarios para las actividades del organismo de evaluación de la conformidad o para que se utilicen dichos productos de TIC para fines personales.

5. Los organismos de evaluación de la conformidad, sus máximos directivos y 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, servicios o procesos de TIC evaluados, ni representarán a las partes que participan en estas actividades. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no efectuarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que estén notificados. Dicha prohibición se aplicará, en particular, a los servicios de consultoría.

6. Si un organismo de evaluación de la conformidad pertenece a una entidad o institución pública o es gestionado por esta, se garantizará y documentará la independencia y la inexistencia de conflictos de interés entre la autoridad nacional de certificación de la seguridad y el organismo de evaluación de la conformidad.

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

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

9. El organismo de evaluación de la conformidad deberá ser capaz de llevar a cabo todas las tareas de evaluación de la conformidad que le hayan sido asignadas en virtud del presente Reglamento, con independencia de si dichas tareas las efectúa el propio organismo o si se realizan en su nombre y bajo su responsabilidad. Cualquier subcontratación o consulta de personal externo se documentará debidamente, no supondrá la participación de intermediarios y será objeto de un acuerdo escrito que regulará, entre otros aspectos, la confidencialidad y el conflicto de intereses. El organismo de evaluación de la conformidad en cuestión asumirá toda la responsabilidad de las tareas desempeñadas.

10. En todo momento, respecto a cada procedimiento de evaluación de la conformidad y cada tipo, categoría o subcategoría de productos, servicios o procesos de TIC, 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 en virtud del artículo 61 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, servicio o proceso de TIC de que se trate y si el proceso de producción es en serie.

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

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

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

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

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

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

13. Se garantizará la imparcialidad del organismo de evaluación de la conformidad, de sus máximos directivos, de las personas responsables de efectuar las actividades de evaluación de la conformidad, y de cualquier subcontratista.

14. La remuneración de los máximos directivos y de las personas responsables de efectuar las actividades de evaluación de la conformidad no dependerá del número de evaluaciones de la conformidad que efectúe ni de los resultados de dichas evaluaciones.

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

16. El organismo de evaluación de la conformidad y su personal, comités, filiales, subcontratistas y cualquier otra entidad o trabajador de organismos externos con los que esté asociado deberán mantener la confidencialidad y observar el secreto profesional acerca de toda la información obtenida en el marco de las tareas de evaluación de la conformidad realizadas en virtud del presente Reglamento o de cualquier disposición de Derecho nacional por la que se aplique, salvo cuando el Derecho de la Unión o de un Estado miembro al que están sometidas dichas personas requiera su divulgación con respecto a las autoridades competentes de los Estados miembros en que realice sus actividades. Se protegerán los derechos de propiedad intelectual. El organismo de evaluación de la conformidad contará con procedimientos documentados por lo que respecta a los requisitos establecidos en el presente punto.

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

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

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

20. Los organismos de evaluación de la conformidad velarán por que los laboratorios de ensayo utilizados con fines de evaluación de la conformidad cumplan los requisitos de la norma pertinente armonizada por el Reglamento (CE) n.º 765/2008 para la acreditación de los laboratorios que realicen ensayos.

DIRECTIVAS

DIRECTIVA (UE) 2019/882 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

sobre los requisitos de accesibilidad de los productos y servicios

(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 [1],

De conformidad con el procedimiento legislativo ordinario [2],

Considerando lo siguiente:

(1) El objetivo de la presente Directiva es contribuir al correcto funcionamiento del mercado interior aproximando las disposiciones legales, reglamentarias y administrativas de los Estados miembros en lo relativo a los requisitos de accesibilidad de determinados productos y servicios, en particular, eliminando y evitando los obstáculos a la libre circulación de determinados productos y servicios accesibles, derivados de las divergencias en los requisitos de accesibilidad en los Estados miembros. Con ello se mejoraría la disponibilidad de productos y servicios accesibles en el mercado interior y aumentaría la accesibilidad de la información pertinente.

(2) La demanda de productos y servicios accesibles es alta y se prevé que el número de personas con discapacidad crecerá de manera importante. Un entorno en el que los productos y servicios son más accesibles permite que la sociedad sea más inclusiva y facilita la vida autónoma de las personas con discapacidad. En este contexto, se ha de tener en cuenta que la discapacidad en la Unión es más preponderante entre las mujeres que entre los hombres.

(3) La presente Directiva define el concepto de personas con discapacidad en consonancia con la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad (en lo sucesivo, «Convención»), adoptada el 13 de diciembre de 2006, en la que la Unión es Parte desde el 21 de enero de 2011 y que ha sido ratificada por todos los Estados miembros. En la Convención se declara que las personas con discapacidad «incluyen a aquellas que tengan deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás». La presente Directiva promueve su participación equitativa, plena y efectiva, mediante la mejora del acceso a los principales productos y servicios que, bien mediante su concepción inicial, bien mediante su posterior adaptación, están dirigidos a las necesidades especiales de las personas con discapacidad.

(4) Otras personas que sufren limitaciones funcionales, como por ejemplo las personas mayores, las mujeres embarazadas o las personas que viajan con equipaje, también se beneficiarían de la presente Directiva. El concepto de «personas con limitaciones funcionales», tal como se menciona en la presente Directiva, engloba a personas que tienen alguna deficiencia física, mental, intelectual o sensorial, alguna deficiencia relacionada con la edad o con otras causas vinculadas al funcionamiento del cuerpo humano, permanente o temporal, que, al interactuar con diversas barreras, limitan su acceso a productos y servicios, dando lugar a una situación que exige una adaptación de tales productos y servicios a sus necesidades particulares.

(5) Las disparidades existentes entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de accesibilidad de productos y servicios para personas con discapacidad constituyen obstáculos a la libre circulación de productos y servicios y distorsionan la competencia efectiva en el mercado interior. En el caso de algunos productos y servicios, es probable que aumenten estas disparidades en la Unión tras la entrada en vigor de la Convención. Los agentes económicos, en particular las pequeñas y medianas empresas (pymes), resultan especialmente afectados por tales obstáculos.

[1] DO C 303 de 19.8.2016, p. 103.

[2] Posición del Parlamento Europeo de 13 de marzo de 2019 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.

(6) Debido a las diferencias entre los requisitos de accesibilidad nacionales, los profesionales, las pymes y las microempresas son especialmente reacios a aventurarse en nuevos proyectos empresariales fuera de los mercados de sus países. Los requisitos de accesibilidad nacionales, o incluso regionales o locales, que han establecido los Estados miembros difieren actualmente tanto en cobertura como en nivel de detalle. Esas diferencias afectan negativamente a la competitividad y al crecimiento, debido a los costes adicionales derivados del desarrollo y la comercialización de productos y servicios accesibles para cada mercado nacional.

(7) Los consumidores de productos y servicios accesibles y de tecnologías de apoyo se encuentran con precios elevados debido a la limitada competencia entre los proveedores. La fragmentación entre las normativas nacionales reduce los beneficios que podría tener compartir experiencias con homólogos nacionales e internacionales para hacer frente a la evolución de la tecnología y de la sociedad.

(8) Por tanto, la aproximación de las medidas nacionales a nivel de la Unión es necesaria para un correcto funcionamiento del mercado interior con objeto de poner fin a la fragmentación del mercado de productos y servicios accesibles, crear economías de escala, facilitar el comercio y la movilidad transfronterizos y ayudar a los agentes económicos a concentrar sus recursos en la innovación en lugar de utilizarlos para cubrir los gastos derivados de una legislación fragmentada en la Unión.

(9) La aplicación de la Directiva 2014/33/UE del Parlamento Europeo y del Consejo ([3]), que regula los ascensores, y del Reglamento (CE) n.º 661/2009 del Parlamento Europeo y del Consejo ([4]), relativo a los transportes, ha demostrado los beneficios de armonizar los requisitos de accesibilidad en el mercado interior.

(10) En la Declaración n.º 22 relativa a las personas discapacitadas, aneja al Tratado de Ámsterdam, la Conferencia de representantes de los gobiernos de los Estados miembros convino en que, al elaborar medidas con arreglo al artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), las instituciones de la Unión deben tener en cuenta las necesidades de las personas discapacitadas.

(11) El objetivo general de la Comunicación de la Comisión de 6 de mayo de 2015, «Una Estrategia para el Mercado Único Digital de Europa», es obtener beneficios económicos y sociales sostenibles de un mercado único digital conectado, facilitando así el comercio y promoviendo el empleo en la Unión. Los consumidores de la Unión aún no disfrutan plenamente de los beneficios en cuanto a precios y ofertas que puede ofrecer ese mercado único, debido a que las transacciones transfronterizas en línea son todavía muy limitadas. La fragmentación limita también la demanda de transacciones transfronterizas de comercio electrónico. Asimismo, se precisa una acción concertada para garantizar que los contenidos electrónicos, los servicios de comunicaciones electrónicas y el acceso a los servicios de comunicación audiovisual estén plenamente disponibles para las personas con discapacidad. Por consiguiente, es necesario armonizar los requisitos de accesibilidad en todo el mercado único digital y garantizar que todos los ciudadanos de la Unión, independientemente de su capacidad, puedan disfrutar de sus beneficios.

(12) Dado que la Unión se ha convertido en Parte en la Convención, sus disposiciones se han convertido en parte integrante del ordenamiento jurídico de la Unión y son vinculantes para las instituciones de la Unión y sus Estados miembros.

(13) La Convención exige a las Partes en ella que adopten las medidas pertinentes para asegurar el acceso de las personas con discapacidad, en igualdad de condiciones con las demás, al entorno físico, el transporte, la información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y las comunicaciones, y a otros servicios e instalaciones abiertos al público o de uso público, tanto en zonas urbanas como rurales. El Comité de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad ha señalado la necesidad de crear un marco legislativo que cuente con parámetros de referencia específicos, aplicables y sujetos a un calendario para supervisar y evaluar la aplicación gradual de la accesibilidad.

(14) La Convención pide a las Partes en ella que emprendan o promuevan la investigación y el desarrollo y que promuevan la disponibilidad y el uso de nuevas tecnologías, entre ellas las tecnologías de la información y de las comunicaciones, así como ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo adecuadas para las personas con discapacidad. La Convención pide asimismo que se dé prioridad a las tecnologías asequibles.

([3]) Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de ascensores y componentes de seguridad para ascensores (DO L 96 de 29.3.2014, p. 251).

([4]) Reglamento (CE) n.º 661/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, relativo a los requisitos de homologación de tipo referentes a la seguridad general de los vehículos de motor, sus remolques y sistemas, componentes y unidades técnicas independientes a ellos destinados (DO L 200 de 31.7.2009, p. 1).

(15) La entrada en vigor de la Convención en los ordenamientos jurídicos de los Estados miembros hace necesario adoptar disposiciones nacionales suplementarias en materia de accesibilidad de los productos y servicios. Sin una actuación por parte de la Unión, tales disposiciones no harían sino aumentar las disparidades entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros.

(16) En consecuencia, es preciso facilitar la aplicación en la Unión de la Convención adoptando disposiciones comunes de la Unión. La presente Directiva también apoya a los Estados miembros en su empeño por cumplir de forma armonizada sus compromisos nacionales, así como sus obligaciones derivadas de la Convención en lo relativo a la accesibilidad.

(17) En consonancia con la Convención, la Comunicación de la Comisión de 15 de noviembre de 2010 titulada «Estrategia Europea sobre Discapacidad 2010-2020: un compromiso renovado para una Europa sin barreras» señala la accesibilidad como uno de sus ocho ámbitos de actuación, indica que se trata de una condición previa básica para la participación en la sociedad y persigue garantizar la accesibilidad de los productos y servicios.

(18) La determinación de los productos y servicios incluidos en el ámbito de aplicación de la presente Directiva se basa en un ejercicio de análisis que se llevó a cabo durante la preparación de la evaluación de impacto, en la cual se determinaron los productos y servicios pertinentes para las personas con discapacidad y en relación con los cuales los Estados miembros han adoptado o van a adoptar probablemente requisitos de accesibilidad nacionales divergentes que alteran el funcionamiento del mercado interior.

(19) A fin de garantizar la accesibilidad de los servicios incluidos en el ámbito de aplicación de la presente Directiva, los productos utilizados en la prestación de aquellos servicios con los que interactúa el consumidor deben ajustarse igualmente a los requisitos de accesibilidad aplicables dispuestos en la presente Directiva.

(20) Aun en el supuesto de que un servicio, o parte de un servicio, se subcontrate a un tercero, la accesibilidad de dicho servicio no debe verse comprometida y los prestadores de servicios deben cumplir las obligaciones de la presente Directiva. Los prestadores de servicios también deben garantizar una formación adecuada y continua de su personal a fin de garantizar que adquiera conocimientos sobre cómo utilizar productos y servicios accesibles. Esa formación ha de incluir cuestiones como el suministro de información, asesoramiento y publicidad.

(21) Los requisitos de accesibilidad deben establecerse de la manera menos gravosa para los agentes económicos y los Estados miembros.

(22) Es necesario especificar requisitos de accesibilidad para la introducción en el mercado de los productos y servicios que entran dentro del ámbito de aplicación de la presente Directiva, a fin de garantizar su libre circulación en el mercado interior.

(23) La presente Directiva debe hacer obligatorios los requisitos de accesibilidad funcional, los cuales deben formularse como objetivos generales. Dichos requisitos deben ser lo bastante precisos para crear obligaciones jurídicamente vinculantes y lo suficientemente detallados para permitir evaluar la conformidad a fin de garantizar el buen funcionamiento del mercado interior de los productos y servicios regulados en la presente Directiva, así como dejar cierto margen de flexibilidad con objeto de permitir la innovación.

(24) La presente Directiva contiene una serie de criterios de rendimiento funcional relacionados con los modos de utilización de los productos y servicios. Dichos criterios no se consideran una alternativa general a los requisitos de accesibilidad establecidos en la presente Directiva y solo deben emplearse en circunstancias muy concretas. Cuando los requisitos de accesibilidad establecidos en la presente Directiva no hagan referencia a una o más de las funciones o características específicas de los productos o servicios, dichos criterios deben aplicarse a tales funciones o características específicas para hacerlos accesibles. Asimismo, en el supuesto de que un requisito de accesibilidad implique requisitos técnicos específicos y de que el producto o servicio ofrezca una solución técnica alternativa para dichos requisitos técnicos, esta solución técnica alternativa debe seguir siendo conforme con los requisitos de accesibilidad correspondientes y dar lugar a una accesibilidad equivalente o mayor mediante la aplicación de los criterios de rendimiento funcional pertinentes.

(25) La presente Directiva debe ser aplicable a los equipos informáticos de uso general de consumo. Para que esos equipos funcionen de manera accesible, sus sistemas operativos también deben ser accesibles. Dichos equipos informáticos se caracterizan por su naturaleza multifuncional y su capacidad para llevar a cabo, con los programas adecuados, la mayoría de las tareas informáticas más habituales solicitadas por los consumidores y están concebidos para ser utilizados por los consumidores. Los ordenadores personales, incluidos los ordenadores de mesa, los ordenadores portátiles, los teléfonos inteligentes y las tabletas, son ejemplos de dichos equipos informáticos. Los

ordenadores especializados integrados en productos electrónicos de consumo no constituyen equipos informáticos de uso general de consumo. La presente Directiva no debe incluir en su ámbito de aplicación, por separado, componentes individuales con funciones específicas, como por ejemplo una tarjeta madre o un chip de memoria, que se utilizan o pueden utilizarse en ese tipo de equipo.

(26) La presente Directiva debe ser aplicable también a los terminales de pago, incluidos tanto sus equipos como sus programas informáticos, y a determinados terminales de autoservicio interactivos, incluidos tanto sus equipos como sus programas informáticos, destinados a ser utilizados para la prestación de servicios contemplados en la presente Directiva: por ejemplo, los cajeros automáticos; las máquinas expendedoras de billetes físicos que den acceso a servicios, como las que expiden títulos de transporte; los dispensadores de turnos en las oficinas bancarias; las máquinas de facturación; y los terminales de autoservicio interactivos que faciliten información, incluidas las pantallas de información interactivas.

(27) No obstante, deben excluirse del ámbito de aplicación de la presente Directiva determinados terminales de autoservicio interactivos que faciliten información instalados como partes integradas de vehículos, aeronaves, buques o material rodante, puesto que forman parte de dichos vehículos, aeronaves, buques o material rodante que no están incluidos en el ámbito de aplicación de la presente Directiva.

(28) La presente Directiva también debe ser aplicable a los servicios de comunicaciones electrónicas, incluidas las comunicaciones de emergencia tal como se definen en la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo ([5]). En la actualidad, las medidas adoptadas por los Estados miembros para facilitar el acceso a las personas con discapacidad son divergentes y no están armonizadas en todo el mercado interior. Garantizar que se apliquen los mismos requisitos de accesibilidad en toda la Unión permitirá realizar economías de escala a los agentes económicos que operen en más de un Estado miembro y facilitará el acceso efectivo a las personas con discapacidad en sus propios Estados miembros y cuando viajen entre Estados miembros. Para que los servicios de comunicaciones electrónicas, incluidas las comunicaciones de emergencia, sean accesibles, los prestadores deben proporcionar, además de la comunicación de voz, servicios de texto en tiempo real y servicios de conversación completa cuando proporcionen apoyo de vídeo, garantizando la sincronización de todos estos medios de comunicación. Como complemento a los requisitos de la presente Directiva, los Estados miembros deben poder determinar un prestador de servicios de retransmisión al que puedan recurrir las personas con discapacidad, de conformidad con la Directiva (UE) 2018/1972.

(29) La presente Directiva armoniza los requisitos de accesibilidad aplicables a los servicios de comunicaciones electrónicas y a los productos conexos y complementa la Directiva (UE) 2018/1972, que establece los requisitos en materia de acceso equivalente y las opciones para los usuarios finales con discapacidad. La Directiva (UE) 2018/1972 también establece requisitos en el marco de las obligaciones de servicio universal sobre el carácter asequible del acceso a internet y de las comunicaciones de voz, así como sobre la asequibilidad y disponibilidad de los equipos terminales conexos y de los equipos y servicios específicos para los consumidores con discapacidad.

(30) La presente Directiva también debe ser aplicable a los equipos terminales de consumo con capacidad informática interactiva que previsiblemente vayan a ser utilizados principalmente para acceder a servicios de comunicaciones electrónicas. A efectos de la presente Directiva, debe considerarse que dichos equipos incluyen equipos utilizados en la configuración para acceder a servicios de comunicaciones electrónicas, como por ejemplo un encaminador o un módem.

(31) A efectos de la presente Directiva, el acceso a los servicios de comunicación audiovisual debe entenderse en el sentido de que los servicios a contenidos audiovisuales son accesibles, así como los mecanismos que permiten a los usuarios con discapacidad utilizar dichas tecnologías de apoyo. Los servicios que dan acceso a servicios de comunicación audiovisual podrían incluir sitios web, aplicaciones en línea, aplicaciones basadas en módulos de conexión, aplicaciones descargables, servicios para dispositivos móviles, incluidas las aplicaciones para dispositivos móviles y reproductores multimedia conexos, así como servicios de televisión conectada. La accesibilidad de los servicios de comunicación audiovisual está regulada por la Directiva 2010/13/UE del Parlamento Europeo y del Consejo ([6]), a excepción de lo relativo a la accesibilidad de las guías electrónicas de programas, que se incluyen en la definición de «servicios que dan acceso a servicios de comunicación audiovisual» a los que es aplicable la presente Directiva.

(32) En el contexto de los servicios de transporte aéreo de viajeros, de transporte de viajeros por autobús, por ferrocarril o por vías navegables, la presente Directiva debe ser aplicable, entre otros, a la difusión de información sobre servicios de transporte incluida la información sobre viajes en tiempo real por medio de sitios web, servicios

([5]) Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

([6]) Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (DO L 95 de 15.4.2010, p. 1).

mediante dispositivos móviles, pantallas de información interactivas y terminales de autoservicio interactivos, requerida por los pasajeros con discapacidad para poder viajar. Ello puede incluir información sobre los servicios y productos de transporte de viajeros del prestador de servicios, información previa al viaje, información durante el viaje e información facilitada cuando se haya cancelado un servicio o se retrase su salida. Otros elementos de información pueden incluir también datos sobre precios y promociones.

(33) La presente Directiva debe ser aplicable asimismo a los sitios web, los servicios para dispositivos móviles, incluidas las aplicaciones para dispositivos móviles concebidas o facilitadas por operadores de servicios de transporte de viajeros en el ámbito de aplicación de la presente Directiva o en su nombre, los servicios de expedición de billetes electrónicos, los billetes electrónicos y los terminales de autoservicio interactivos.

(34) La determinación del ámbito de aplicación de la presente Directiva con respecto a los servicios de transporte aéreo de viajeros, de transporte de viajeros por autobús, por ferrocarril y por vías navegables debe basarse en la legislación sectorial existente en el ámbito de los derechos de los pasajeros. En aquellos casos en los que la presente Directiva no se aplique a determinados tipos de servicios de transporte, los Estados miembros deben animar a los prestadores de servicios a aplicar los requisitos pertinentes en materia de accesibilidad dispuestos en la presente Directiva.

(35) La Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo ([7]) ya establece obligaciones para que los organismos del sector público que prestan servicios de transporte, incluidos los servicios de transporte urbanos y suburbanos y los servicios de transporte regionales, hagan accesibles sus sitios web. La presente Directiva contiene exenciones aplicables a las microempresas que prestan servicios, incluidos los servicios de transporte urbanos y suburbanos y los servicios de transporte regionales. Asimismo, la presente Directiva incluye obligaciones para garantizar que los sitios web de comercio electrónico sean accesibles. Puesto que la presente Directiva contiene obligaciones exigibles a la gran mayoría de prestadores privados de servicios de transporte de que hagan accesibles sus sitios web en lo relativo a la venta en línea de billetes, no es necesario establecer en la presente Directiva otros requisitos para los sitios web de prestadores de servicios de transporte urbanos y suburbanos y prestadores de servicios de transporte regionales.

(36) Determinados elementos de los requisitos de accesibilidad, en particular respecto a la difusión de información que establece la presente Directiva, ya están regulados por el Derecho de la Unión vigente en el ámbito del transporte de viajeros. Cabe citar elementos del Reglamento (CE) n.º 261/2004 del Parlamento Europeo y del Consejo ([8]), del Reglamento (CE) n.º 1107/2006 del Parlamento Europeo y del Consejo ([9]), del Reglamento (CE) n.º 1371/2007 del Parlamento Europeo y del Consejo ([10]), del Reglamento (UE) n.º 1177/2010 del Parlamento Europeo y del Consejo ([11]) y del Reglamento (UE) n.º 181/2011 del Parlamento Europeo y del Consejo ([12]). Cabe citar asimismo actos pertinentes adoptados sobre la base de la Directiva 2008/57/CE del Parlamento Europeo y del Consejo ([13]). Por coherencia normativa, los requisitos de accesibilidad que figuran en dichos Reglamentos y actos deben seguir aplicándose como antes. Sin embargo, los requisitos adicionales de la presente Directiva complementan los requisitos actuales, mejorando el funcionamiento del mercado interior en el sector del transporte y beneficiando a las personas con discapacidad.

(37) La presente Directiva no debe ser aplicable a determinados elementos de los servicios de transporte, que se efectúan fuera del territorio de los Estados miembros aunque el servicio esté dirigido al mercado de la Unión. Por lo que respecta a dichos elementos, un operador de servicios de transporte de viajeros solo debe estar obligado a garantizar que se cumplen los requisitos de la presente Directiva con respecto a la parte del servicio ofrecida dentro del territorio de la Unión. No obstante, en el caso del transporte aéreo, las compañías aéreas de la Unión deben garantizar que se cumplan los requisitos aplicables de la presente Directiva también en el caso de los vuelos

([7]) Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público (DO L 327 de 2.12.2016, p. 1).

([8]) Reglamento (CE) n.º 261/2004 del Parlamento Europeo y del Consejo, de 11 de febrero de 2004, por el que se establecen normas comunes sobre compensación y asistencia a los pasajeros aéreos en caso de denegación de embarque y de cancelación o gran retraso de los vuelos, y se deroga el Reglamento (CEE) n.º 295/91 (DO L 46 de 17.2.2004, p. 1).

([9]) Reglamento (CE) n.º 1107/2006 del Parlamento Europeo y del Consejo, de 5 de julio de 2006, sobre los derechos de las personas con discapacidad o movilidad reducida en el transporte aéreo (DO L 204 de 26.7.2006, p. 1).

([10]) Reglamento (CE) n.º 1371/2007 del Parlamento Europeo y del Consejo, de 23 de octubre de 2007, sobre los derechos y las obligaciones de los viajeros de ferrocarril (DO L 315 de 3.12.2007, p. 14).

([11]) Reglamento (UE) n.º 1177/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, sobre los derechos de los pasajeros que viajan por mar y por vías navegables y por el que se modifica el Reglamento (CE) n.º 2006/2004 (DO L 334 de 17.12.2010, p. 1).

([12]) Reglamento (UE) n.º 181/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, sobre los derechos de los viajeros de autobús y autocar y por el que se modifica el Reglamento (CE) n.º 2006/2004 (DO L 55 de 28.2.2011, p. 1).

([13]) Directiva 2008/57/CE del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la interoperabilidad del sistema ferroviario dentro de la Comunidad (DO L 191 de 18.7.2008, p. 1).

procedentes de un aeropuerto situado en un tercer país con destino a un aeropuerto situado en el territorio de un Estado miembro. Además, todas las compañías aéreas, incluso aquellas que no dispongan de una licencia de la Unión, deben garantizar que se cumplan los requisitos aplicables de la presente Directiva en los casos de vuelos que salgan del territorio de la Unión hacia el de un tercer país.

(38) Se debe alentar a las administraciones municipales a que integren en sus planes de movilidad urbana sostenible la accesibilidad sin barreras a los servicios de transporte urbanos y a que publiquen periódicamente listas de buenas prácticas en lo que se refiere a la accesibilidad sin barreras a los transportes públicos y la movilidad urbanos.

(39) El Derecho de la Unión en materia de servicios bancarios y financieros tiene por objetivo proteger a los consumidores de dichos servicios en toda la Unión y proporcionarles información, pero no incluye requisitos de accesibilidad. Con el fin de permitir que las personas con discapacidad utilicen esos servicios en toda la Unión, también cuando se prestan a través de sitios web y de servicios para dispositivos móviles, incluidas las aplicaciones para dispositivos móviles, tomen decisiones bien informadas y tengan la tranquilidad de que están adecuadamente protegidas, en condiciones de igualdad con los demás consumidores, y con el fin de garantizar unas condiciones de competencia equitativas para los prestadores de servicios, la presente Directiva debe establecer requisitos de accesibilidad comunes para algunos servicios bancarios y financieros prestados a los consumidores.

(40) Asimismo, se deben aplicar los requisitos de accesibilidad adecuados a los métodos de identificación, la firma electrónica y los servicios de pago, pues son necesarios para que los consumidores realicen transacciones bancarias.

(41) Los archivos de libros electrónicos se basan en una codificación informática electrónica que permite la divulgación y consulta de una obra intelectual fundamentalmente textual y gráfica. El grado de precisión de dicha codificación determina la accesibilidad de los archivos de libros electrónicos, en particular en lo relativo a la cualificación de los diferentes elementos constitutivos de la obra y la descripción normalizada de su estructura. La interoperabilidad en términos de accesibilidad debe optimizar la compatibilidad de dichos archivos con los agentes de usuario y con las tecnologías de apoyo actuales y futuras. Las características específicas de obras especiales como los tebeos, los libros infantiles y los libros de arte deben tenerse en cuenta a la luz de todos los requisitos de accesibilidad aplicables. Unos requisitos de accesibilidad divergentes entre los Estados miembros harían difícil que editores y otros agentes económicos obtuvieran provecho de las ventajas del mercado interior, podrían plantear problemas de interoperabilidad con los lectores electrónicos y limitarían el acceso a los consumidores con discapacidad. En el contexto de los libros electrónicos, el concepto de «prestador de servicios» podría incluir a los editores y demás agentes económicos que intervienen en la distribución de libros electrónicos.

Se reconoce que las personas con discapacidad siguen enfrentándose a obstáculos para acceder a los contenidos protegidos por derechos de autor y derechos afines, y que ya se han adoptado algunas medidas para abordar esta situación, por ejemplo, mediante la adopción de la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo ([14]) y del Reglamento (UE) 2017/1563 del Parlamento Europeo y del Consejo ([15]), y se reconoce que en el futuro podrían adoptarse otras medidas a este respecto.

(42) La presente Directiva define el concepto de «servicios de comercio electrónico» como los servicios prestados a distancia, a través de sitios web y servicios para dispositivos móviles, por medios electrónicos y a petición individual de un consumidor, al objeto de celebrar un contrato con el consumidor. A efectos de la definición anterior hay que entender por: «a distancia», un servicio prestado sin que las partes estén presentes de forma simultánea; «por medios electrónicos», un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético; «a petición individual de un consumidor», un servicio prestado a petición individual. Dada la importancia creciente de los servicios de comercio electrónico y su carácter altamente tecnológico, es importante contar con requisitos armonizados en relación con su accesibilidad.

([14]) Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017, sobre ciertos usos permitidos de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, y por la que se modifica la Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (DO L 242 de 20.9.2017, p. 6).

([15]) Reglamento (UE) 2017/1563 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017, sobre el intercambio transfronterizo entre la Unión y terceros países de ejemplares en formato accesible de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos (DO L 242 de 20.9.2017, p. 1).

(43) Las obligaciones de accesibilidad de los servicios de comercio electrónico de la presente Directiva deben aplicarse a la venta en línea de cualquier producto o servicio y, por tanto, también deben aplicarse a la venta de un producto o servicio sujeto por sí mismo a la presente Directiva.

(44) Las medidas relativas a la accesibilidad de las respuestas a las comunicaciones de emergencia deben adoptarse sin menoscabar ni afectar a la organización de los servicios de emergencia, que sigue siendo competencia exclusiva de los Estados miembros.

(45) Con arreglo a la Directiva (UE) 2018/1972, los Estados miembros han de velar por que el acceso a los servicios de emergencia para los usuarios finales con discapacidad esté disponible a través de las comunicaciones de emergencia y sea equivalente a aquel del que disfrutan otros usuarios finales, de conformidad con el Derecho de la Unión por el que se armonizan los requisitos de accesibilidad a productos y servicios. La Comisión y las autoridades nacionales de reglamentación u otras autoridades competentes han de adoptar las medidas adecuadas para garantizar que, en sus desplazamientos a otro Estado miembro, los usuarios finales con discapacidad puedan acceder a los servicios de emergencia en igualdad de condiciones respecto al resto de usuarios finales y, a ser posible, sin necesidad de registro previo. Estas medidas procuran garantizar la interoperabilidad entre los Estados miembros y han de basarse en la mayor medida posible en las normas o las especificaciones europeas pertinentes establecidas de conformidad con el artículo 39 de la Directiva (UE) 2018/1972. Dichas medidas no impiden a los Estados miembros adoptar requisitos adicionales para perseguir los objetivos establecidos en dicha Directiva. Como alternativa al cumplimiento de los requisitos de accesibilidad relativos a las respuestas a las comunicaciones de emergencia para los usuarios con discapacidad establecidos en la presente Directiva, los Estados miembros deben poder determinar un tercero prestador de servicios de retransmisión para que lo utilicen las personas con discapacidad con el fin de comunicarse con el punto de respuesta de seguridad pública, hasta que dichos puntos de respuesta de seguridad pública puedan utilizar servicios de comunicaciones electrónicas a través de protocolos de internet para garantizar la accesibilidad de las respuestas a las comunicaciones de emergencia. En cualquier caso, no cabe interpretar que las obligaciones de la presente Directiva limitan o reducen obligación alguna que favorezca a usuarios finales con discapacidad, incluidas obligaciones equiparables en materia de acceso a los servicios de comunicaciones electrónicas y de emergencia, así como de accesibilidad que se establecen en la Directiva (UE) 2018/1972.

(46) La Directiva (UE) 2016/2102 determina los requisitos de accesibilidad para los sitios web y aplicaciones para dispositivos móviles de los organismos públicos, y otros aspectos conexos, en particular los requisitos relativos a la conformidad de los correspondientes sitios web y aplicaciones para dispositivos móviles. Sin embargo, dicha Directiva contiene una lista específica de excepciones. Excepciones similares son pertinentes a efectos de la presente Directiva. Algunas actividades que se realizan a través de los sitios web y aplicaciones para dispositivos móviles de los organismos públicos, como los servicios de transporte de viajeros o los servicios de comercio electrónico, incluidas en el ámbito de aplicación de la presente Directiva, deben cumplir también los requisitos de accesibilidad aplicables que se establecen en ella, para garantizar así que la venta en línea de productos y servicios sea accesible a las personas con discapacidad independientemente de que el vendedor sea un agente económico público o privado. Los requisitos de accesibilidad establecidos en la presente Directiva deben adaptarse a los requisitos de la Directiva (UE) 2016/2102, a pesar de las diferencias que existen, por ejemplo, en materia de seguimiento, presentación de informes y aplicación.

(47) Los cuatro principios de la accesibilidad a los sitios web y a las aplicaciones para dispositivos móviles, tal como los emplea la Directiva (UE) 2016/2102, son: perceptibilidad, en el sentido de que la información y los componentes de la interfaz de usuario deben presentarse a este de manera que pueda percibirlos; operabilidad, en el sentido de que los componentes y la navegación de la interfaz de usuario deben poder utilizarse; comprensibilidad, en el sentido de que la información y el funcionamiento de la interfaz de usuario deben ser comprensibles; y robustez, en el sentido de que los contenidos deben ser suficientemente sólidos para poder ser interpretados de forma fiable por una gran variedad de agentes de usuario, incluidas las tecnologías de apoyo. Tales principios son también pertinentes para la presente Directiva.

(48) Los Estados miembros deben adoptar todas las medidas adecuadas para garantizar que, si los productos y servicios objeto de la presente Directiva cumplen los requisitos de accesibilidad aplicables, su libre circulación en la Unión no se vea obstaculizada por razones relacionadas con los requisitos de accesibilidad.

(49) En algunas situaciones, los requisitos comunes de accesibilidad del entorno construido facilitarían la libre circulación de los servicios conexos y de las personas con discapacidad. Por ello, la presente Directiva debe permitir a los Estados miembros incluir el entorno construido utilizado en la prestación de los servicios incluidos en su ámbito de aplicación, garantizando el cumplimiento de los requisitos de accesibilidad establecidos en el anexo III.

(50) Debe lograrse la accesibilidad a través de la supresión y evitación sistemáticas de las barreras, preferiblemente a través de un planteamiento de diseño universal o «diseño para todos», que contribuya a garantizar el acceso de las personas con discapacidad en condiciones de igualdad con los demás. De acuerdo con la Convención, por ese planteamiento «se entenderá el diseño de productos, entornos, programas y servicios que puedan utilizar todas las personas, en la mayor medida posible, sin necesidad de adaptación ni diseño especializado». De conformidad con la

Convención, el «"diseño universal" no excluirá las ayudas técnicas para grupos particulares de personas con discapacidad, cuando se necesiten». Además, la accesibilidad no debe excluir la realización de adaptaciones razonables cuando así lo exija el Derecho de la Unión o el nacional. La accesibilidad y el diseño universal deben interpretarse en consonancia con la observación general n.º 2(2014) sobre el artículo 9: accesibilidad, redactada por el Comité sobre los Derechos de las Personas con Discapacidad.

(51) Los productos y servicios que entran en el ámbito de aplicación de la presente Directiva no entran automáticamente en el ámbito de aplicación de la Directiva 93/42/CEE del Consejo ([16]). Sin embargo, es posible que algunas tecnologías de apoyo que son productos sanitarios entren en el ámbito de aplicación de dicha Directiva.

(52) En la Unión, la mayoría de los empleos los proporcionan pymes o microempresas. Estas, a pesar de tener una importancia clave para el crecimiento futuro, muy a menudo se enfrentan a obstáculos y barreras en el desarrollo de sus productos o servicios, en particular en el contexto transfronterizo. Por tanto, es necesario facilitar el trabajo de las pymes y las microempresas armonizando las disposiciones nacionales sobre accesibilidad, al tiempo que se mantienen las salvaguardias necesarias.

(53) Para que las microempresas y las pymes puedan disfrutar de la presente Directiva, tienen que cumplir realmente las condiciones de la Recomendación 2003/361/CE de la Comisión ([17]), y la jurisprudencia aplicable, con el fin de evitar la elusión de sus normas.

(54) Con el fin de garantizar la coherencia del Derecho de la Unión, la presente Directiva debe basarse en la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo ([18]), pues se refiere a productos ya regulados en otros actos de la Unión, reconociendo al mismo tiempo las características específicas de los requisitos de accesibilidad establecidos en la presente Directiva.

(55) Todos los agentes económicos que entren en el ámbito de aplicación de la presente Directiva y que intervengan en la cadena de suministro y distribución deben garantizar que solo comercializan productos conformes con la presente Directiva. Debe aplicarse esa misma exigencia a los agentes económicos que presten servicios. Es necesario establecer un reparto claro y proporcionado de las obligaciones correspondientes al papel de cada agente económico en el proceso de suministro y distribución.

(56) Los agentes económicos deben ser responsables de la conformidad de los productos y servicios, en relación con la función que desempeñen respectivamente en la cadena de suministro, de modo que puedan garantizar un nivel elevado de protección de la accesibilidad y garantizar la competencia leal dentro del mercado de la Unión.

(57) Las obligaciones de la presente Directiva deben aplicarse igualmente a los agentes económicos de los sectores público y privado.

(58) Dado que el fabricante dispone de conocimientos específicos sobre el diseño y el proceso de producción, es el más indicado para llevar a cabo todo el procedimiento de evaluación de la conformidad. Aunque la responsabilidad de la conformidad de los productos sigue siendo del fabricante, las autoridades de vigilancia del mercado deben desempeñar un papel clave a la hora de comprobar si los productos que se comercializan en la Unión se fabrican con arreglo al Derecho de la Unión.

(59) Los importadores y distribuidores deben intervenir en las tareas de vigilancia del mercado realizadas por las autoridades nacionales y participar activamente facilitando a las autoridades competentes toda la información necesaria sobre el producto en cuestión.

(60) Los importadores deben garantizar que los productos procedentes de terceros países que entren en el mercado de la Unión cumplan la presente Directiva y, en particular, que los fabricantes hayan llevado a cabo los procedimientos de evaluación de la conformidad adecuados con respecto a esos productos.

(61) Al introducir un producto en el mercado, los importadores deben indicar en el producto su nombre, nombre comercial registrado o marca registrada y la dirección de contacto.

([16]) Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios (DO L 169 de 12.7.1993, p. 1).
([17]) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).
([18]) Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

(62) Los distribuidores deben asegurarse de que su forma de tratar el producto no afecta negativamente a la conformidad de este con los requisitos de accesibilidad establecidos en la presente Directiva.

(63) Cualquier agente económico que introduzca un producto en el mercado con su nombre o marca comercial o modifique un producto ya introducido en el mercado, de manera que pueda afectar al cumplimiento de los requisitos aplicables, debe considerarse que es el fabricante y asumir las obligaciones del fabricante.

(64) Por motivos de proporcionalidad, los requisitos de accesibilidad solo deben aplicarse en la medida en que no impongan una carga desproporcionada al agente económico concreto, o en la medida en que no exijan un cambio significativo en los productos o servicios que pueda dar lugar a una modificación sustancial a la luz de la presente Directiva. Se deben establecer, no obstante, mecanismos de control para verificar si existe el derecho a excepciones respecto de la aplicabilidad de los requisitos de accesibilidad.

(65) La presente Directiva debe seguir el principio de «pensar primero a pequeña escala» y tener en cuenta las cargas administrativas a las que se enfrentan las pymes. Debe establecer disposiciones sencillas de evaluación de la conformidad y establecer cláusulas de salvaguardia para los agentes económicos, en lugar de ofrecer excepciones y exenciones generales para esas empresas. Por consiguiente, al adoptar las disposiciones sobre la selección y aplicación de los procedimientos de evaluación de la conformidad más adecuados, debe tenerse en cuenta la situación de las pymes y la obligación de evaluar la conformidad de los requisitos de accesibilidad debe limitarse en tal medida que no plantee una carga desproporcionada a las pymes. Además, las autoridades de vigilancia del mercado deben funcionar de una manera proporcionada al tamaño de las empresas y su tipo de producción, en series pequeñas o no en serie, sin crear innecesariamente obstáculos para las pymes ni comprometer la protección del interés público.

(66) En casos excepcionales, cuando el cumplimiento de los requisitos de accesibilidad establecidos en la presente Directiva vaya a suponer una carga desproporcionada para los agentes económicos, solo se debe exigir a estos que cumplan esos requisitos en la medida en que no les supongan una carga desproporcionada. En tales casos, que deben estar debidamente justificados, no sería razonablemente posible que un agente económico aplicase plenamente uno o más de los requisitos de accesibilidad. No obstante, el agente económico debe garantizar que un servicio o producto incluido en el ámbito de aplicación de la presente Directiva sea lo más accesible posible aplicando dichos requisitos en la medida en que no supongan una carga desproporcionada. Deben aplicarse plenamente los requisitos de accesibilidad que, a juicio del agente económico, no supongan una carga desproporcionada. Las excepciones al cumplimiento de uno o varios requisitos de accesibilidad debidas a la carga desproporcionada que suponen no deben ir más allá de lo estrictamente necesario para limitar esa carga respecto al producto o servicio en particular de que se trate en cada caso. Por medidas que impondrían una carga desproporcionada deben entenderse aquellas medidas que impondrían una carga organizativa o financiera excesiva adicional al agente económico, teniendo en cuenta al mismo tiempo el probable beneficio resultante para las personas con discapacidad en consonancia con los criterios establecidos en la presente Directiva. Deberán definirse criterios basados en estas consideraciones de modo que los agentes económicos y las autoridades competentes puedan comparar diferentes situaciones y evaluar de manera sistemática la existencia de una carga desproporcionada. Al valorar hasta qué punto no pueden satisfacerse los requisitos porque supondrían una carga desproporcionada, solo deben tenerse en cuenta razones legítimas. No deben considerarse razones legítimas la falta de prioridad, de tiempo o de conocimientos.

(67) La evaluación general de una carga desproporcionada debe realizarse recurriendo a los criterios establecidos en el anexo VI. El agente económico debe documentar la evaluación de la carga desproporcionada teniendo en cuenta los criterios pertinentes. Los prestadores de servicios deben volver a hacer la evaluación de la carga desproporcionada al menos cada cinco años.

(68) Los agentes económicos deben informar a las autoridades correspondientes de que se han basado en las disposiciones de la presente Directiva relativas a la modificación sustancial o a la carga desproporcionada. Solo a petición de las autoridades correspondientes deben proporcionar los agentes económicos una copia de la evaluación, con la explicación de los motivos por los que su producto o servicio no es plenamente accesible, así como la prueba de que evitarlo supondría una carga desproporcionada o una modificación sustancial, o ambas.

(69) Aunque, basándose en la evaluación requerida, un prestador de servicios concluya que supondría una carga desproporcionada exigir que todos los terminales de autoservicio, utilizados para la prestación de los servicios incluidos en el ámbito de la presente Directiva, cumplan los requisitos de accesibilidad establecidos en la presente Directiva, el prestador de servicios debe seguir aplicando tales requisitos en la medida en que no supongan una carga desproporcionada. En consecuencia, el prestador de servicios debe evaluar en qué medida un grado limitado de accesibilidad de todos los terminales de autoservicio o un número limitado de terminales de autoservicio totalmente accesibles le permitiría evitar una carga desproporcionada que, de otro modo, se le impondría, y se le debe exigir que cumpla con los requisitos de accesibilidad establecidos en la presente Directiva solo en esa medida.

(70) Las microempresas se distinguen de todas las demás empresas por sus recursos humanos limitados, su reducido volumen de negocios anual o balance anual total. Por lo tanto, en general, la carga que supone para las microempresas el cumplimiento de los requisitos de accesibilidad absorbe una parte de sus recursos humanos y financieros mayor que en otras empresas y es más probable que represente una parte desproporcionada de los costes. Una parte significativa de los costes para las microempresas se debe a la formalización o conservación de documentación y registros para demostrar el cumplimiento de los diferentes requisitos establecidos en el Derecho de la Unión. Por lo tanto, si bien todos los agentes económicos a los que es aplicable la presente Directiva deben poder evaluar la proporcionalidad del cumplimiento de los requisitos de accesibilidad establecidos en ella y deben cumplirlos solo en la medida en que no sean desproporcionados, la exigencia de este tipo de evaluación a las microempresas que presten servicios constituiría en sí misma una carga desproporcionada. Por consiguiente, los requisitos y obligaciones de la presente Directiva no deben aplicarse a las microempresas que presten servicios incluidos en su ámbito de aplicación.

(71) Respecto de las microempresas dedicadas a productos incluidos en el ámbito de aplicación de la presente Directiva, los requisitos y obligaciones de la presente Directiva deben ser menos exigentes para reducir la carga administrativa.

(72) Si bien algunas microempresas están exentas de las obligaciones de la presente Directiva, conviene animar a todas las microempresas a fabricar, importar y distribuir productos, y prestar servicios, que cumplan los requisitos de accesibilidad establecidos en la presente Directiva, para aumentar la competitividad y el crecimiento potencial de dichas empresas en el mercado interior. Por tanto, los Estados miembros deben proporcionar orientaciones y herramientas a las microempresas con el fin de facilitar la aplicación de las disposiciones nacionales de transposición de la presente Directiva.

(73) Todos los agentes económicos deben actuar de manera responsable y de conformidad plena con los requisitos jurídicos aplicables cuando introduzcan en el mercado o comercialicen productos o presten servicios.

(74) A fin de facilitar la evaluación de la conformidad con los requisitos de accesibilidad aplicables es necesario establecer una presunción de conformidad para los productos y servicios que cumplan las normas armonizadas voluntarias que se adopten con arreglo al Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([19]) a fin de elaborar especificaciones técnicas detalladas de estos requisitos. La Comisión ya ha presentado a los organismos europeos de normalización diversas solicitudes de normalización relativas a la accesibilidad, como los mandatos de normalización M/376, M/473 y M/420, que serían pertinentes para elaborar normas armonizadas.

(75) El Reglamento (UE) n.º 1025/2012 establece un procedimiento de objeciones formales sobre aquellas normas armonizadas que se considere que no cumplen los requisitos de la presente Directiva.

(76) Las normas europeas deben estar orientadas al mercado, tener en cuenta el interés público, así como los objetivos de actuación claramente enunciados en la petición dirigida por la Comisión a una o más organizaciones europeas de normalización para que elaboren normas armonizadas, y estar basadas en el consenso. En ausencia de normas armonizadas y cuando sea necesario a efectos de armonización del mercado interior, la Comisión debe poder adoptar, en determinados casos, actos de ejecución que establezcan especificaciones técnicas para los requisitos de accesibilidad establecidos en la presente Directiva. Conviene limitar a esos casos el recurso a las especificaciones técnicas. La Comisión debe poder adoptar especificaciones técnicas, por ejemplo, cuando esté bloqueado el proceso de normalización debido a una falta de consenso entre las partes interesadas o cuando haya demoras indebidas en el establecimiento de una norma armonizada, por ejemplo porque no se logra la calidad exigida. La Comisión debe dejar suficiente tiempo entre la aprobación de una petición de elaboración de normas armonizadas dirigida a una o más organizaciones europeas de normalización y la adopción de una especificación técnica relativa al mismo requisito de accesibilidad. No debe permitirse que la Comisión adopte especificaciones técnicas si no ha intentado previamente que los requisitos de accesibilidad queden cubiertos mediante el sistema europeo de normalización, excepto si la Comisión puede demostrar que las especificaciones técnicas respetan los requisitos establecidos en el anexo II del Reglamento (UE) n.º 1025/2012.

(77) Con miras a establecer, de la manera más eficiente posible, normas y especificaciones técnicas armonizadas que cumplan los requisitos de accesibilidad establecidos en la presente Directiva para los productos y servicios, la Comisión debe involucrar en el proceso, cuando sea factible, a las organizaciones centrales europeas que representan a las personas con discapacidad y a todas las partes interesadas pertinentes.

([19]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

(78) Para garantizar el acceso efectivo a la información con fines de vigilancia del mercado, la información necesaria para declarar la conformidad con todos los actos de la Unión aplicables debe ponerse a disposición en una declaración UE de conformidad única. Con objeto de reducir la carga administrativa para los agentes económicos, estos deben poder incluir en la declaración UE de conformidad única todas las correspondientes declaraciones de conformidad individuales.

(79) Para la evaluación de la conformidad de los productos, la presente Directiva debe seguir el módulo A (Control interno de la producción) del anexo II de la Decisión n.º 768/2008/CE, que permite a los agentes económicos demostrar, y a las autoridades competentes garantizar, que los productos comercializados son conformes con los requisitos de accesibilidad sin imponer una carga injustificada.

(80) Cuando lleven a cabo la vigilancia del mercado de los productos y verifiquen la conformidad de los servicios, las autoridades también deben verificar las evaluaciones de la conformidad, en particular si se efectuó correctamente la evaluación de modificación sustancial o de carga desproporcionada. Cuando lleven a cabo sus funciones, las autoridades deben realizarlas en cooperación con las personas con discapacidad y las organizaciones que las representan a ellas y sus intereses.

(81) En el caso de los servicios, la información necesaria para evaluar la conformidad con los requisitos de accesibilidad establecidos en la presente Directiva debe facilitarse en las condiciones generales o en un documento equivalente, sin perjuicio lo dispuesto en la Directiva 2011/83/UE del Parlamento Europeo y del Consejo ([20]).

(82) El marcado CE, que indica la conformidad de un producto con los requisitos de accesibilidad establecidos en la presente Directiva, es el resultado visible de todo un proceso que comprende la evaluación de la conformidad en sentido amplio. La presente Directiva debe ajustarse a los principios generales que rigen el marcado CE con arreglo al Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([21]), por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos. Además de efectuar la declaración UE de conformidad, el fabricante debe informar a los consumidores, de una manera económica, sobre la accesibilidad de sus productos.

(83) De conformidad con el Reglamento (CE) n.º 765/2008, al colocar el marcado CE en un producto el fabricante declara que el producto cumple todos los requisitos de accesibilidad aplicables y que él asume la plena responsabilidad al respecto.

(84) De conformidad con la Decisión n.º 768/2008/CE, los Estados miembros son responsables de garantizar en sus territorios una vigilancia del mercado de los productos sólida y eficaz, y deben conferir competencias y recursos suficientes a sus autoridades de vigilancia del mercado.

(85) Los Estados miembros deben comprobar la conformidad de los servicios con las obligaciones de la presente Directiva y hacer un seguimiento de las quejas o los informes sobre no conformidad para garantizar que se han tomado medidas correctoras.

(86) Cuando corresponda, la Comisión puede adoptar, en consulta con los interesados, orientaciones no vinculantes que contribuyan a la coordinación entre las autoridades de vigilancia del mercado y las autoridades responsables de verificar la conformidad de los servicios. La Comisión y los Estados miembros deben poder poner en marcha iniciativas con el fin de compartir los recursos y experiencias de las autoridades.

(87) Los Estados miembros deben garantizar que las autoridades de vigilancia del mercado y las autoridades responsables de verificar la conformidad de los servicios comprueban la conformidad de los agentes económicos con los criterios recogidos en el anexo VI, con arreglo a los capítulos VIII y IX. Los Estados miembros deben poder designar un organismo especializado para ejercer las obligaciones propias de las autoridades de vigilancia del mercado o de las autoridades responsables de verificar la conformidad de los servicios en virtud de la presente Directiva. Los Estados miembros deben poder decidir que las competencias de dicho organismo especializado se limiten al ámbito de aplicación de la presente Directiva o a determinadas partes de ella, sin perjuicio de las obligaciones de los Estados miembros en virtud del Reglamento (CE) n.º 765/2008.

([20]) Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo (DO L 304 de 22.11.2011, p. 64).

([21]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 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 (DO L 218 de 13.8.2008, p. 30).

(88) Debe establecerse un procedimiento de salvaguardia, aplicable en caso de desacuerdo entre los Estados miembros sobre las medidas adoptadas por uno de ellos, según el cual las partes interesadas sean informadas de las medidas previstas en relación con productos que no cumplan los requisitos de accesibilidad establecidos en la presente Directiva. El procedimiento de salvaguardia debe permitir a las autoridades de vigilancia del mercado, en cooperación con los agentes económicos pertinentes, actuar en una fase más temprana respecto a estos productos.

(89) Si los Estados miembros y la Comisión convienen en que una medida adoptada por un Estado miembro está justificada, no debe exigirse otra intervención de la Comisión, excepto en los casos en que la no conformidad pueda atribuirse a las insuficiencias en las normas armonizadas o en las especificaciones técnicas.

(90) Las Directivas 2014/24/UE ([22]) y 2014/25/UE ([23]) del Parlamento Europeo y del Consejo, sobre contratación pública, en las que se definen procedimientos para la adjudicación de contratos públicos y concursos de proyectos para determinados suministros (productos), servicios y obras, establecen que, para toda contratación que esté destinada a ser utilizada por personas físicas, ya sea el público en general o el personal del poder o entidad adjudicadores, las especificaciones técnicas se redactarán, salvo en casos debidamente justificados, de manera que se tengan en cuenta los criterios de accesibilidad para las personas con discapacidad o el diseño para todos los usuarios. Además, dichas Directivas obligan a que, cuando se adopten requisitos imperativos de accesibilidad mediante un acto jurídico de la Unión, las especificaciones técnicas se definan, en lo que respecta a los criterios de accesibilidad para las personas con discapacidad o el diseño para todos los usuarios, por referencia a ellos. La presente Directiva debe establecer requisitos de accesibilidad obligatorios respecto de los productos y servicios que regula. Respecto de los productos y servicios que no entren dentro del ámbito de aplicación de la presente Directiva, los requisitos de accesibilidad establecidos en la presente Directiva no son obligatorios. No obstante, el uso de dichos requisitos de accesibilidad para cumplir las obligaciones pertinentes establecidas en actos de la Unión distintos de la presente Directiva facilitaría la aplicación de la accesibilidad y contribuiría a la seguridad jurídica y a la aproximación de los requisitos de accesibilidad en toda la Unión. No se debe impedir a las autoridades que establezcan requisitos de accesibilidad que vayan más allá de lo establecido en el anexo I de la presente Directiva.

(91) La presente Directiva no debe alterar la naturaleza obligatoria o voluntaria de las disposiciones sobre accesibilidad contenidas en otros actos de la Unión.

(92) La presente Directiva solo debe ser aplicable a los procedimientos de contratación respecto de los cuales se haya enviado una convocatoria de licitación o, si no se ha previsto una convocatoria de licitación, cuando la autoridad o entidad contratante haya iniciado el procedimiento de contratación tras la fecha de aplicación de la presente Directiva.

(93) A fin de garantizar la correcta aplicación de la presente Directiva, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE, por lo que respecta a: una mayor precisión de los requisitos de accesibilidad que, por su propia naturaleza, no pueden surtir el efecto deseado si no son objeto de una mayor precisión en actos jurídicos vinculantes de la Unión; el cambio del período durante el cual los agentes económicos han de poder identificar a cualquier agente económico que les haya suministrado un producto o al cual hayan suministrado un producto; y más detalles sobre los criterios pertinentes que deba tener en cuenta el agente económico para evaluar si el cumplimiento de los requisitos de accesibilidad supondrían una carga desproporcionada. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([24]). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(94) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución en lo que respecta a las especificaciones técnicas. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([25]).

([22]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

([23]) Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE (DO L 94 de 28.3.2014, p. 243).

([24]) DO L 123 de 12.5.2016, p. 1.

([25]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(95) Los Estados miembros deben asegurarse de que existan medios adecuados y efectivos para garantizar el cumplimiento de la presente Directiva y establecer, por lo tanto, mecanismos de control adecuados, tales como un control *a posteriori* por parte de las autoridades de vigilancia del mercado, con el fin de verificar que la exención respecto de la aplicación de los requisitos de accesibilidad está justificada. Al tramitar las quejas relativas a la accesibilidad, los Estados miembros deben cumplir el principio general de buena administración, y en particular la obligación de los funcionarios de garantizar que se tome una decisión sobre cada queja en un plazo razonable.

(96) A fin de facilitar la ejecución uniforme de la presente Directiva, la Comisión debe establecer un grupo de trabajo formado por las pertinentes autoridades e interesados para facilitar el intercambio de información y mejores prácticas y prestar asesoramiento. Se debe fomentar la cooperación entre las autoridades y los interesados pertinentes, en particular las personas con discapacidad y las organizaciones que las representan, entre otras cosas para mejorar la coherencia en la aplicación de las disposiciones de la presente Directiva relativas a los requisitos de accesibilidad y para controlar la ejecución de las disposiciones sobre modificaciones sustanciales y carga desproporcionada.

(97) Habida cuenta del marco jurídico existente en relación con las vías de recurso en los ámbitos a los que se aplican las Directivas 2014/24/UE y 2014/25/UE, las disposiciones de la presente Directiva relativas a la vigilancia del cumplimiento y las sanciones no deben ser aplicables a los procedimientos de contratación sujetos a las obligaciones impuestas por la presente Directiva. Tal exclusión se entiende sin perjuicio de las obligaciones de los Estados miembros, derivadas de los Tratados, de adoptar todas las medidas necesarias para garantizar la aplicación y la eficacia del Derecho de la Unión.

(98) Las sanciones deben ser adecuadas en relación con el carácter de las infracciones y con las circunstancias, de manera que no sirvan como alternativa al cumplimiento por los agentes económicos de la obligación de que sus productos o servicios sean accesibles.

(99) Los Estados miembros deben velar por que, de conformidad con el Derecho vigente de la Unión, se hayan establecido mecanismos alternativos de resolución de controversias que permitan resolver cualquier presunto incumplimiento de la presente Directiva antes de que se interponga una demanda ante los tribunales o los organismos administrativos competentes.

(100) De conformidad con la Declaración política conjunta, de 28 de septiembre de 2011, de los Estados miembros y de la Comisión sobre los documentos explicativos ([26]), los Estados miembros se han comprometido a adjuntar a la notificación de las medidas de transposición, cuando esté justificado, 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 dichos documentos está justificada.

(101) A fin de conceder a los prestadores de servicios el tiempo suficiente para adaptarse a los requisitos de la presente Directiva, es necesario disponer un período de transición de cinco años a partir de la fecha de aplicación de la presente Directiva, durante el cual no se exija que los productos usados para la prestación de un servicio que fueron introducidos en el mercado con anterioridad a esa fecha cumplan los requisitos de accesibilidad establecidos en la presente Directiva, a menos que sean reemplazados por los prestadores de servicios durante el período de transición. Habida cuenta del coste y el largo ciclo de vida de los terminales de autoservicio, es conveniente disponer que, en aquellos casos en los que estos terminales se empleen para la prestación de servicios, puedan seguir utilizándose hasta el final de su vida útil, siempre y cuando no sean sustituidos durante ese período, aunque sin superar los veinte años.

(102) Los requisitos de accesibilidad establecidos en la presente Directiva deben aplicarse a los productos que se introduzcan en el mercado y a los servicios prestados tras la fecha de aplicación de las medidas nacionales de transposición de la presente Directiva, en particular los productos usados y de segunda mano importados de un tercer país que se introduzcan en el mercado después de esa fecha.

(103) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en especial, por la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»). En particular, su objetivo es garantizar el pleno respeto de los derechos de las personas con discapacidad a beneficiarse de medidas diseñadas para garantizar su autonomía, su integración social y profesional y su participación en la vida de la comunidad, y fomentar la aplicación de los artículos 21, 25 y 26 de la Carta.

(104) Dado que el objetivo de la presente Directiva, a saber, la eliminación de los obstáculos a la libre circulación de determinados productos y servicios accesibles, para contribuir al correcto funcionamiento del mercado interior, no puede ser alcanzado de manera suficiente por los Estados miembros, pues requiere la armonización de disposiciones diferentes actualmente vigentes en sus respectivos sistemas jurídicos, sino que, debido a que se definen requisitos comunes de accesibilidad y disposiciones para el funcionamiento del mercado interior, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dicho objetivo.

([26]) DO C 369 de 17.12.2011, p. 14.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

El objetivo de la presente Directiva es contribuir al correcto funcionamiento del mercado interior mediante la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en lo relativo a los requisitos de accesibilidad exigibles a determinados productos y servicios, en particular eliminando y evitando los obstáculos a la libre circulación de productos y servicios derivados de las divergencias en los requisitos de accesibilidad en los Estados miembros.

Artículo 2

Ámbito de aplicación

1. La presente Directiva es aplicable a los siguientes productos que se introduzcan en el mercado con posterioridad al 28 de junio de 2025:

a) equipos informáticos de uso general de consumo y sistemas operativos para dichos equipos informáticos;

b) los siguientes terminales de autoservicio:

i) terminales de pago,

ii) los siguientes terminales de autoservicio dedicados a la prestación de servicios contemplados en la presente Directiva:

— cajeros automáticos,

— máquinas expendedoras de billetes,

— máquinas de facturación,

— terminales de autoservicio interactivos que faciliten información, con exclusión de los terminales instalados como partes integradas de vehículos, aeronaves, buques o material rodante;

c) equipos terminales de consumo con capacidad informática interactiva, utilizados para la prestación de servicios de comunicaciones electrónicas;

d) equipos terminales de consumo con capacidad de informática interactiva, utilizados para acceder a servicios de comunicación audiovisual, y

e) lectores electrónicos.

2. Sin perjuicio de lo dispuesto en el artículo 32, la presente Directiva es aplicable a los siguientes servicios que se presten a los consumidores con posterioridad al 28 de junio de 2025:

a) servicios de comunicaciones electrónicas, a excepción de los servicios de transmisión utilizados para la prestación de servicios de máquina a máquina;

b) servicios que proporcionan acceso a los servicios de comunicación audiovisual;

c) los siguientes elementos de los servicios de transporte aéreo de viajeros, de transporte de viajeros por autobús, por ferrocarril y por vías navegables, salvo los servicios de transporte urbanos, suburbanos y regionales para los cuales serán de aplicación únicamente los elementos del inciso v):

i) sitios web,

ii) servicios mediante dispositivos móviles, incluidas las aplicaciones para dispositivos móviles,

iii) billetes electrónicos y servicios de expedición de billetes electrónicos,

iv) distribución de información sobre servicios de transporte, en particular información sobre viajes en tiempo real; en lo que respecta a las pantallas informativas, se limitará a las pantallas interactivas situadas dentro del territorio de la Unión, y

v) terminales de servicio interactivos situados dentro del territorio de la Unión, excepto los instalados como partes integradas en vehículos, aeronaves, buques y material rodante empleados para la prestación de cualquier parte de dichos servicios de transporte de viajeros;

d) servicios bancarios para consumidores;

e) libros electrónicos y sus programas especializados, y

f) servicios de comercio electrónico.

3. La presente Directiva es aplicable a las respuestas a las comunicaciones de emergencia al número único europeo de emergencia «112».

4. La presente Directiva no es aplicable a los siguientes contenidos de sitios web y aplicaciones para dispositivos móviles:

a) contenidos multimedia pregrabados de base temporal publicados antes del 28 de junio de 2025;

b) formatos de archivo de ofimática publicados antes del 28 de junio de 2025;

c) servicios de mapas y cartografía en línea, cuando la información esencial se proporcione de manera accesible digitalmente en el caso de mapas destinados a fines de navegación;

d) contenidos de terceros que no estén financiados ni desarrollados por el agente económico en cuestión ni estén bajo su control;

e) contenidos de sitios web y aplicaciones para dispositivos móviles considerados como archivos, en el sentido de que contienen únicamente contenidos que no se actualizan ni editan después del 28 de junio de 2025.

5. La presente Directiva se entenderá sin perjuicio de la Directiva (UE) 2017/1564 y del Reglamento (UE) 2017/1563.

Artículo 3

Definiciones

A efectos de la presente Directiva, se entenderá por:

1) «personas con discapacidad»: aquellas personas que tienen deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás;

2) «producto»: sustancia, preparado o mercancía producidos por medio de un proceso de fabricación, que no sean alimentos, piensos, plantas ni animales vivos, productos de origen humano ni productos de origen vegetal o animal directamente relacionados con su futura reproducción;

3) «servicio»: un servicio tal como se define en el artículo 4, punto 1, de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo ([27]);

4) «prestador de servicios»: toda persona física o jurídica que presta un servicio en el mercado de la Unión o que hace ofertas para prestar dicho servicio a los consumidores de la Unión;

5) «servicios de comunicación audiovisual»: los servicios definidos en el artículo 1, apartado 1, letra a), de la Directiva 2010/13/UE;

6) «servicios que dan acceso a servicios de comunicación audiovisual»: servicios transmitidos por redes de comunicaciones electrónicas que se utilizan para identificar servicios de comunicación audiovisual, para seleccionarlos, recibir información sobre ellos y para visualizarlos, así como cualquier característica presentada, como subtítulos para sordos y deficientes auditivos, descripción de audio, subtítulos hablados e interpretación de lenguaje de señas, que resulten de la aplicación de medidas para hacer los servicios accesibles según lo previsto en el artículo 7 de la Directiva 2010/13/UE, e incluyen las guías electrónicas de programas;

7) «equipo terminal de consumo con capacidad informática interactiva, utilizado para acceder a servicios de comunicación audiovisual»: todo equipo cuya principal finalidad es facilitar acceso a los servicios de comunicación audiovisual;

([27]) Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior (DO L 376 de 27.12.2006, p. 36).

8) «servicio de comunicaciones electrónicas»: servicio de comunicaciones electrónicas tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2018/1972;

9) «servicio de conversación total»: un servicio de conversación total tal como se define en el artículo 2, punto 35, de la Directiva (UE) 2018/1972;

10) «punto de respuesta de seguridad pública» o «PSAP»: un punto de respuesta de seguridad pública o PSAP tal como se define en el artículo 2, punto 36, de la Directiva (UE) 2018/1972;

11) «PSAP más apropiado»: un PSAP más apropiado tal como se define en el artículo 2, punto 37, de la Directiva (UE) 2018/1972;

12) «comunicación de emergencia»: una comunicación de emergencia tal como se define en el artículo 2, punto 38, de la Directiva (UE) 2018/1972;

13) «servicio de emergencia»: un servicio de emergencia tal como se define en el artículo 2, punto 39, de la Directiva (UE) 2018/1972;

14) «texto en tiempo real»: una forma de conversación de texto en situaciones de punto a punto o conferencia con múltiples puntos en la que el texto es introducido de tal forma que la comunicación es percibida por el usuario como continua en forma de carácter por carácter;

15) «comercialización»: todo suministro, remunerado o gratuito, de un producto para su distribución, consumo o utilización en el mercado de la Unión en el transcurso de una actividad comercial;

16) «introducción en el mercado»: primera comercialización de un producto en el mercado de la Unión;

17) «fabricante»: toda persona física o jurídica que fabrica un producto o que manda diseñar o fabricar un producto y lo comercializa con su nombre o marca comercial;

18) «representante autorizado»: toda persona física o jurídica establecida en la Unión que ha recibido un mandato escrito de un fabricante para actuar en su nombre en tareas específicas;

19) «importador»: toda persona física o jurídica establecida en la Unión que introduce un producto de un tercer país en el mercado de la Unión;

20) «distribuidor»: toda persona física o jurídica de la cadena de suministro, distinta del fabricante o el importador, que comercializa un producto;

21) «agente económico»: el fabricante, el representante autorizado, el importador, el distribuidor o el prestador de servicios;

22) «consumidor»: toda persona física que compra un producto o es destinatario de un servicio con fines ajenos a su actividad comercial o empresarial, su oficio o su profesión;

23) «microempresa»: una empresa que emplea a menos de 10 personas y cuyo volumen de negocios anual no supera los 2 millones de euros o cuyo balance anual total no supera los 2 millones de euros;

24) «pequeñas y medianas empresas» o «pymes»: empresas que emplean a menos de 250 personas y cuyo volumen de negocios anual no supera los 50 millones de euros o cuyo balance anual total no supera los 43 millones de euros, excluidas las microempresas;

25) «norma armonizada»: una norma armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012;

26) «especificación técnica»: una especificación técnica tal como se define en el artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012, que proporciona un medio para cumplir los requisitos de accesibilidad aplicables a un producto o servicio;

27) «retirada»: cualquier medida encaminada a prevenir la comercialización de un producto que se encuentra en la cadena de suministro;

28) «servicios bancarios para consumidores»: la prestación de los siguientes servicios bancarios y financieros a los consumidores:

a) contratos de crédito que se regulan en la Directiva 2008/48/CE del Parlamento Europeo y del Consejo ([28]) o en la Directiva 2014/17/UE del Parlamento Europeo y del Consejo ([29]);

b) servicios definidos en los puntos 1, 2, 4 y 5 de la sección A y en los puntos 1, 2, 4 y 5 de la sección B del anexo I de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo ([30]);

c) servicios de pago, tal como se definen en el artículo 4, punto 3, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo ([31]);

d) servicios vinculados a la cuenta de pago tal como se definen en el artículo 2, punto 6, de la Directiva 2014/92/UE del Parlamento Europeo y del Consejo ([32]), y

e) el dinero electrónico tal como se define en el artículo 2, punto 2, de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo ([33]);

29) «terminal de pago»: un dispositivo cuya principal finalidad es permitir realizar pagos haciendo uso de instrumentos de pago tal como se definen en el artículo 4, punto 14, de la Directiva (UE) 2015/2366 en un punto físico de venta pero no en un entorno virtual;

30) «servicios de comercio electrónico»: los servicios prestados a distancia a través de sitios web y servicios para dispositivos móviles, por medios electrónicos y a petición individual de un consumidor, al objeto de celebrar un contrato con el consumidor;

31) «servicios de transporte aéreo de viajeros»: los servicios comerciales de transporte aéreo de viajeros tal como se definen en el artículo 2, letra l), del Reglamento (CE) n.º 1107/2006, para salir de un aeropuerto, en situaciones de tránsito en él o al llegar a él, cuando el aeropuerto esté situado en el territorio de un Estado miembro, incluidos los vuelos procedentes de un aeropuerto situado en un tercer país con destino a un aeropuerto situado en el territorio de un Estado miembro cuando una compañía aérea de la Unión preste los servicios;

32) «servicios de transporte de viajeros por autobús»: los servicios incluidos en el artículo 2, apartados 1 y 2, del Reglamento (UE) n.º 181/2011;

33) «servicios de transporte de viajeros por ferrocarril»: todos los servicios de ferrocarril para viajeros a que se refiere el artículo 2, apartado 1, del Reglamento (CE) n.º 1371/2007, a excepción de los servicios a que se refiere el artículo 2, apartado 2, del citado Reglamento;

34) «servicios de transporte de viajeros por vías navegables»: los servicios incluidos en el artículo 2, apartado 1, del Reglamento (UE) n.º 1177/2010, a excepción de los servicios a que se refiere el artículo 2, apartado 2, del citado Reglamento;

35) «servicios de transporte urbanos y suburbanos»: los servicios urbanos y suburbanos tal como se definen en el artículo 3, punto 6, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo ([34]); ahora bien, a efectos de la presente Directiva, solo incluye los siguientes modos de transporte: ferrocarril, autobús y autocar, metro, tranvía y trolebús;

([28]) Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo (DO L 133 de 22.5.2008, p. 66).

([29]) Directiva 2014/17/UE del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, sobre los contratos de crédito celebrados con los consumidores para bienes inmuebles de uso residencial y por la que se modifican las Directivas 2008/48/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 (DO L 60 de 28.2.2014, p. 34).

([30]) Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349).

([31]) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35).

([32]) Directiva 2014/92/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la comparabilidad de las comisiones conexas a las cuentas de pago, el traslado de cuentas de pago y el acceso a cuentas de pago básicas (DO L 257 de 28.8.2014, p. 214).

([33]) Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, p. 7).

([34]) Directiva 2012/34/UE del Parlamento Europeo y del Consejo, de 21 de noviembre de 2012, por la que se establece un espacio ferroviario europeo único (DO L 343 de 14.12.2012, p. 32).

36) «servicios de transporte regionales»: los servicios regionales tal como se definen en el artículo 3, punto 7, de la Directiva 2012/34/UE; ahora bien, a efectos de la presente Directiva, solo incluye los siguientes modos de transporte: ferrocarril, autobús y autocar, metro, tranvía y trolebús;

37) «tecnología de apoyo»: cualquier artículo, equipo, servicio o sistema de productos, incluidos los programas, que se utilice para aumentar, mantener, sustituir o mejorar las capacidades funcionales de las personas con discapacidad, o para paliar o compensar deficiencias, limitaciones de la actividad o restricciones de la participación;

38) «sistema operativo»: un programa que, entre otras cosas, gestiona la interfaz del equipo periférico, programa tareas, distribuye la memoria y presenta una interfaz predeterminada al usuario cuando no se está ejecutando ningún programa de aplicación, incluida una interfaz gráfica de usuario, independientemente de si dicho programa forma parte del equipo informático de uso general de consumo o si se trata de un programa independiente destinado a ejecutarse en el equipo informático de uso general de consumo; ahora bien, se excluyen el cargador del sistema operativo, el sistema básico de entrada/salida u otros microprogramas necesarios al arrancar el sistema o instalar el sistema operativo;

39) «equipos informáticos de uso general de consumo»: una combinación de equipos que forma un ordenador completo, caracterizado por su naturaleza multifuncional, su capacidad para llevar a cabo, con los programas adecuados, la mayoría de las tareas informáticas más habituales solicitadas por los consumidores y concebido para ser utilizado por ellos, e incluye los ordenadores personales, en particular los ordenadores de sobremesa, los ordenadores portátiles, los teléfonos inteligentes y las tabletas;

40) «capacidad informática interactiva»: una funcionalidad de apoyo para la interacción entre el usuario y el dispositivo que posibilita el procesamiento y la transmisión de datos, voz o vídeo o cualquier combinación de estos;

41) «libro electrónico y sus programas especializados»: un servicio consistente en el suministro de archivos digitales que contienen una versión electrónica de un libro a la que se puede acceder, por la que se puede navegar y que se puede leer y utilizar, así como de los programas, incluidos los servicios para dispositivos móviles, incluidas las aplicaciones para dispositivos móviles, especializados en el acceso, la navegación, la lectura y el uso de esos archivos digitales, excluidos los programas comprendidos en la definición del punto 42;

42) «lector electrónico»: un equipo especializado, incluidos tanto el aparato como el programa, utilizado para acceder a archivos de libros electrónicos, navegar por ellos, leerlos y utilizarlos;

43) «billetes electrónicos»: todo sistema en el que el derecho a viajar, ya sea en forma de billete de viaje individual o múltiple, abono de viaje o crédito de viaje, se almacena electrónicamente en una tarjeta de transporte física o en otro dispositivo, en lugar de imprimirse en un billete de papel;

44) «servicios de expedición de billetes electrónicos»: todo sistema en que los billetes de transporte de los viajeros se adquieren en línea a través de un dispositivo con capacidad informática interactiva y se envían al comprador en formato electrónico, a fin de que pueda imprimirlos en papel o mostrarlos en un dispositivo móvil con capacidad informática interactiva cuando vaya a viajar.

CAPÍTULO II

Requisitos de accesibilidad y libre circulación

Artículo 4

Requisitos de accesibilidad

1. Los Estados miembros garantizarán, de conformidad con los apartados 2, 3 y 5 del presente artículo y a reserva del artículo 14, que los agentes económicos solo introduzcan en el mercado los productos y solo presten los servicios que cumplan los requisitos de accesibilidad que figuran en el anexo I.

2. Todos los productos deberán cumplir los requisitos de accesibilidad que figuran en la sección I del anexo I.

Todos los productos, a excepción de los terminales de autoservicio, deberán cumplir los requisitos de accesibilidad que figuran en la sección II del anexo I.

3. Sin perjuicio de lo dispuesto en el apartado 5 del presente artículo, todos los servicios, salvo los servicios de transporte urbanos y suburbanos y los servicios de transporte regionales, deberán cumplir los requisitos de accesibilidad que figuran en la sección III del anexo I.

Sin perjuicio de lo dispuesto en el apartado 5 del presente artículo, todos los servicios deberán cumplir los requisitos de accesibilidad que figuran en la sección IV del anexo I.

4. Los Estados miembros podrán decidir, en función de las condiciones nacionales, si el entorno construido utilizado por los clientes de los servicios objeto de la presente Directiva deben cumplir los requisitos de accesibilidad que figuran en el anexo III, con el fin de maximizar su uso por personas con discapacidad.

5. Las microempresas que presten servicios estarán exentas de cumplir los requisitos de accesibilidad a que se refiere el apartado 3 del presente artículo y cualquier obligación relativa al cumplimiento de dichos requisitos.

6. Los Estados miembros proporcionarán orientaciones y herramientas a las microempresas con el fin de facilitar la aplicación de las medidas nacionales de transposición de la presente Directiva. Los Estados miembros elaborarán dichas herramientas en concertación con las partes interesadas pertinentes.

7. Los Estados miembros podrán informar a los agentes económicos de los ejemplos indicativos, que figuran en el anexo II, relativos a posibles medidas que contribuyen al cumplimiento de los requisitos de accesibilidad del anexo I.

8. Los Estados miembros garantizarán que la respuesta a las comunicaciones de emergencia al número único europeo de emergencia «112» por el PSAP más apropiado cumpla los requisitos de accesibilidad específicos que figuran en la sección V del anexo I de la manera más adecuada a la estructuración de los dispositivos nacionales de emergencia.

9. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 26 para completar el anexo I, precisando en mayor medida los requisitos de accesibilidad que, por su propia naturaleza, no pueden surtir el efecto deseado si no son objeto de una mayor precisión en actos jurídicos vinculantes de la Unión, como los requisitos relativos a la interoperabilidad.

Artículo 5

Derecho de la Unión vigente en el ámbito del transporte de viajeros

Se considerará que los servicios que cumplan los requisitos de suministro de información accesible y de información sobre accesibilidad establecidos en los Reglamentos (CE) n.º 261/2004, (CE) n.º 1107/2006, (CE) n.º 1371/2007, (UE) n.º 1177/2010 y (UE) n.º 181/2011 y que cumplan los actos pertinentes adoptados sobre la base de la Directiva 2008/57/CE satisfacen los requisitos correspondientes de la presente Directiva. Cuando la presente Directiva establezca requisitos adicionales a los previstos en dichos Reglamentos y actos, los requisitos adicionales se aplicarán plenamente.

Artículo 6

Libre circulación

Los Estados miembros no impedirán, por razones relacionadas con los requisitos de accesibilidad, la comercialización de productos ni la prestación de servicios, en su territorio, que cumplan la presente Directiva.

CAPÍTULO III

Obligaciones de los agentes económicos que guardan relación con los productos

Artículo 7

Obligaciones de los fabricantes

1. Cuando introduzcan sus productos en el mercado, los fabricantes se asegurarán de que estos se han diseñado y fabricado de conformidad con los requisitos de accesibilidad aplicables de la presente Directiva.

2. Los fabricantes elaborarán la documentación técnica con arreglo al anexo IV y aplicarán o mandarán aplicar el procedimiento de evaluación de la conformidad establecido en dicho anexo.

Cuando se haya demostrado que el producto cumple los requisitos de accesibilidad aplicables mediante ese procedimiento, los fabricantes elaborarán una declaración UE de conformidad y colocarán el marcado CE.

3. Los fabricantes conservarán la documentación técnica y la declaración UE de conformidad durante cinco años después de la introducción del producto en el mercado.

4. Los fabricantes se asegurarán de que existen procedimientos para que la producción en serie mantenga su conformidad con la presente Directiva. Deberán tomarse debidamente en consideración los cambios en el diseño o las características del producto y los cambios en las normas armonizadas, o en las especificaciones técnicas, con arreglo a las cuales se declara la conformidad de un producto.

5. Los fabricantes se asegurarán de que sus productos llevan un número de tipo, lote o serie o cualquier otro elemento que permita su identificación o, si el tamaño o la naturaleza del producto no lo permite, de que la información requerida figura en el embalaje o envase o en un documento que acompañe al producto.

6. Los fabricantes indicarán su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto en el producto o, cuando no sea posible, en su embalaje o envase o en un documento que lo acompañe. La dirección deberá indicar un punto único en el que pueda contactarse con el fabricante. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios finales y las autoridades de vigilancia del mercado.

7. Los fabricantes garantizarán que el producto vaya acompañado de las instrucciones y la información relativa a la seguridad en una lengua fácilmente comprensible para los consumidores y otros usuarios finales, según lo que decida el Estado miembro de que se trate. Dichas instrucciones e información, así como cualquier etiquetado, serán claros, comprensibles e inteligibles.

8. Los fabricantes que consideren o tengan motivos para pensar que un producto que han introducido en el mercado no es conforme con la presente Directiva adoptarán inmediatamente las medidas correctoras necesarias para hacerlo conforme, o, si procede, retirarlo del mercado. Además, cuando el producto no cumpla los requisitos de accesibilidad establecidos en la presente Directiva, los fabricantes informarán inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que hayan comercializado el producto y darán detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas. En tales casos, los fabricantes llevarán un registro de los productos que no cumplan los requisitos de accesibilidad aplicables y de las quejas correspondientes.

9. Previa solicitud motivada de una autoridad nacional competente, los fabricantes le facilitarán toda la información y documentación necesarias para demostrar la conformidad del producto, en una lengua fácilmente comprensible para dicha autoridad. Cooperarán con dicha autoridad, a petición suya, en cualquier acción emprendida para subsanar el incumplimiento de los requisitos de accesibilidad aplicables de los productos que hayan introducido en el mercado, en particular haciendo que los productos cumplan los requisitos de accesibilidad aplicables.

Artículo 8

Representantes autorizados

1. Los fabricantes podrán designar, mediante mandato escrito, a un representante autorizado.

Las obligaciones establecidas en el artículo 7, apartado 1, y la elaboración de la documentación técnica no formarán parte del mandato del representante autorizado.

2. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del fabricante. El mandato deberá permitir al representante autorizado realizar como mínimo las tareas siguientes:

a) mantener la declaración UE de conformidad y la documentación técnica a disposición de las autoridades de vigilancia del mercado durante cinco años;

b) previa solicitud motivada de una autoridad nacional competente, facilitar a dicha autoridad toda la información y documentación necesarias para demostrar la conformidad del producto;

c) cooperar con las autoridades nacionales competentes, a petición de estas, en cualquier acción emprendida para subsanar el incumplimiento de los requisitos de accesibilidad aplicables de los productos objeto de su mandato.

Artículo 9

Obligaciones de los importadores

1. Los importadores solo introducirán en el mercado productos conformes.

2. Antes de introducir un producto en el mercado, los importadores se asegurarán de que el fabricante haya aplicado el procedimiento de evaluación de la conformidad establecido en el anexo IV. Se asegurarán de que el fabricante haya elaborado la documentación técnica exigida por dicho anexo, de que el producto lleve el marcado CE y vaya acompañado de los documentos necesarios y de que el fabricante haya cumplido los requisitos de etiquetado establecidos en el artículo 7, apartados 5 y 6.

3. Si un importador considera o tiene motivos para pensar que un producto no cumple los requisitos de accesibilidad aplicables de la presente Directiva, no lo introducirá en el mercado hasta que el producto sea conforme. Además, en los casos en los que el producto no cumpla los requisitos de accesibilidad aplicables, el importador informará al fabricante y a las autoridades de vigilancia del mercado al respecto.

4. Los importadores indicarán su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto en el producto o, cuando no sea posible, en su embalaje o envase o en un documento que lo acompañe. Los datos de contacto figurarán en una lengua fácilmente comprensible para los usuarios finales y las autoridades de vigilancia del mercado.

5. Los importadores garantizarán que el producto vaya acompañado de las instrucciones y la información relativa a la seguridad en una lengua fácilmente comprensible para los consumidores y otros usuarios finales, según lo que decida el Estado miembro de que se trate.

6. Los importadores se asegurarán de que, mientras un producto esté bajo su responsabilidad, las condiciones de almacenamiento o transporte no comprometan el cumplimiento de los requisitos de accesibilidad aplicables.

7. Durante un período de cinco años los importadores mantendrán una copia de la declaración UE de conformidad a disposición de las autoridades de vigilancia del mercado y se asegurarán de que, previa petición, la documentación técnica se pueda poner a disposición de dichas autoridades.

8. Los importadores que consideren o tengan motivos para pensar que un producto que han introducido en el mercado no es conforme con la presente Directiva adoptarán inmediatamente las medidas correctoras necesarias para hacerlo conforme o, si procede, retirarlo del mercado. Además, cuando el producto no cumpla los requisitos de accesibilidad aplicables, los importadores informarán inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que hayan comercializado el producto y darán detalles, en particular, sobre el incumplimiento y las medidas correctoras adoptadas. En tales casos, los importadores llevarán un registro de los productos que no cumplan los requisitos de accesibilidad aplicables y de las quejas correspondientes.

9. Previa solicitud motivada de una autoridad nacional competente, los importadores le facilitarán toda la información y documentación necesarias para demostrar la conformidad de un producto en una lengua fácilmente comprensible para dicha autoridad. Cooperarán con dicha autoridad, a petición suya, en cualquier acción emprendida para subsanar el incumplimiento de los requisitos de accesibilidad aplicables de los productos que hayan introducido en el mercado.

Artículo 10

Obligaciones de los distribuidores

1. Al comercializar un producto, los distribuidores actuarán con la debida diligencia respecto a los requisitos de la presente Directiva.

2. Antes de comercializar un producto, los distribuidores comprobarán que el producto lleve el marcado CE, que vaya acompañado de los documentos necesarios y de las instrucciones y la información relativa a la seguridad en una lengua fácilmente comprensible para los consumidores y otros usuarios finales del Estado miembro en el que vaya a ser comercializado, y que el fabricante y el importador hayan cumplido los requisitos establecidos en el artículo 7, apartados 5 y 6, y en el artículo 9, apartado 4, respectivamente.

3. Si un distribuidor considera o tiene motivos para pensar que un producto no es conforme con los requisitos de accesibilidad aplicables de la presente Directiva, no lo comercializará hasta que sea conforme. Además, cuando el producto no cumpla los requisitos de accesibilidad aplicables, el distribuidor informará de ello al fabricante o al importador y a las autoridades de vigilancia del mercado.

4. Los distribuidores se asegurarán de que, mientras un producto esté bajo su responsabilidad, las condiciones de almacenamiento o transporte no comprometan el cumplimiento de los requisitos de accesibilidad aplicables.

5. Los distribuidores que consideren o tengan motivos para pensar que un producto que han comercializado no es conforme con la presente Directiva se asegurarán de que se adopten las medidas correctoras necesarias para hacerlo conforme o, si procede, retirarlo del mercado. Además, cuando el producto no cumpla los requisitos de accesibilidad aplicables, los distribuidores informarán inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que hayan comercializado el producto y darán detalles, en particular, sobre el incumplimiento y las medidas correctoras adoptadas.

6. Previa solicitud motivada de la autoridad nacional competente, los distribuidores le facilitarán toda la información y documentación necesarias para demostrar la conformidad de un producto. Cooperarán con dicha autoridad, a petición suya, en cualquier acción emprendida para subsanar el incumplimiento de los requisitos de accesibilidad aplicables de los productos que hayan comercializado.

Artículo 11

Casos en los que las obligaciones de los fabricantes se aplican a los importadores y los distribuidores

A los efectos de la presente Directiva, tendrá la consideración de fabricante y, por consiguiente, estará sujeto a las obligaciones del fabricante con arreglo al artículo 7, el importador o distribuidor que introduzca un producto en el mercado con su nombre o marca o que modifique un producto ya introducido en el mercado de tal modo que pueda quedar afectado el cumplimiento de los requisitos de la presente Directiva.

Artículo 12

Identificación de los agentes económicos que guardan relación con los productos

1. Previa solicitud, los agentes económicos a que se refieren los artículos 7 a 10 identificarán ante las autoridades de vigilancia del mercado a los siguientes agentes:

a) a cualquier otro agente económico que les haya suministrado un producto;

b) a cualquier otro agente económico al que hayan suministrado un producto.

2. Los agentes económicos a que se refieren los artículos 7 a 10 podrán presentar la información a que se refiere el apartado 1 del presente artículo durante un período de cinco años después de la fecha en la que se les haya suministrado el producto y durante un período de cinco años después de la fecha en la que ellos hayan suministrado el producto.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 26, para modificar la presente Directiva a fin de modificar el período a que se refiere el apartado 2 del presente artículo para productos concretos. Dicho período modificado será superior a cinco años y será proporcional a la vida económicamente útil del producto de que se trate.

CAPÍTULO IV

Obligaciones de los prestadores de servicios

Artículo 13

Obligaciones de los prestadores de servicios

1. Los prestadores de servicios garantizarán que diseñan y prestan servicios de conformidad con los requisitos de accesibilidad establecidos en la presente Directiva.

2. Los prestadores de servicios elaborarán la información necesaria de conformidad con el anexo V y explicarán de qué manera sus servicios cumplen los requisitos de accesibilidad aplicables. La información se pondrá a disposición del público en formato escrito y oral, y también de forma que sea accesible para las personas con discapacidad. Los prestadores de servicios deberán conservar la información mientras el servicio esté en funcionamiento.

3. Sin perjuicio de lo dispuesto en el artículo 32, los prestadores de servicios se asegurarán de que existan procedimientos que garanticen que la prestación de servicios siga siendo conforme con los requisitos de accesibilidad aplicables. Los prestadores de servicios tendrán debidamente en cuenta los cambios en las características de la prestación del servicio, los cambios en los requisitos de accesibilidad aplicables y los cambios en las normas armonizadas o en las especificaciones técnicas en relación con las cuales se declara que el servicio cumple los requisitos de accesibilidad.

4. En caso de no conformidad, los prestadores de servicios adoptarán las medidas correctoras necesarias para hacer conforme el servicio con los requisitos de accesibilidad aplicables. Además, cuando el servicio no cumpla los requisitos de accesibilidad aplicables, los prestadores de servicios informarán inmediatamente de ello a las autoridades nacionales competentes de los Estados miembros en los que prestan el servicio y darán detalles, en particular, sobre el incumplimiento y las medidas correctoras adoptadas.

5. Previa solicitud motivada de una autoridad competente, los prestadores de servicios le facilitarán toda la información necesaria para demostrar la conformidad del servicio con los requisitos de accesibilidad aplicables. Cooperarán con dicha autoridad, a petición de esta, en cualquier acción emprendida para hacer conforme el servicio con dichos requisitos.

CAPÍTULO V

Modificación sustancial de productos o servicios y carga desproporcionada sobre los agentes económicos

Artículo 14

Modificación sustancial y carga desproporcionada

1. Los requisitos de accesibilidad a que se refiere el artículo 4 solo serán aplicables en la medida en que su cumplimiento:

a) no exija un cambio significativo en un producto o servicio cuyo resultado sea la modificación sustancial de su naturaleza básica, y

b) no provoque la imposición de una carga desproporcionada sobre los agentes económicos afectados.

2. Los agentes económicos llevarán a cabo una evaluación de si el cumplimiento de los requisitos de accesibilidad a que se refiere el artículo 4 originarían una modificación sustancial o, con arreglo a los criterios correspondientes que figuran en el anexo VI, impondrían una carga desproporcionada, según lo dispuesto en el apartado 1 del presente artículo.

3. Los agentes económicos documentarán la evaluación a que se refiere el apartado 2. Los agentes económicos conservarán todos los resultados pertinentes durante un período de cinco años calculado a partir de la última comercialización de un producto o después de la última prestación de un servicio, según corresponda. A instancia de las autoridades de vigilancia del mercado o de las autoridades responsables de verificar la conformidad de los servicios, según el caso, los agentes económicos les facilitarán una copia de la evaluación a que se refiere el apartado 2.

4. Como excepción a lo dispuesto en el apartado 3, las microempresas que guarden relación con los productos estarán exentas del requisito de documentar su evaluación. No obstante, si una autoridad de vigilancia del mercado lo solicita, las microempresas que guarden relación con los productos y que hayan optado por acogerse a lo dispuesto en el apartado 1 facilitarán a la autoridad la información pertinente a efectos de la evaluación a que se refiere el apartado 2.

5. Los prestadores de servicios que invoquen la letra b) del apartado 1 renovarán, respecto de cada categoría o tipo de servicio, su evaluación sobre si una carga es desproporcionada:

a) cuando se modifique el servicio ofrecido, o

b) cuando así lo soliciten las autoridades responsables de verificar la conformidad de los servicios, y

c) en cualquier caso, cada cinco años.

6. Cuando los agentes económicos reciban financiación procedente de fuentes distintas de los recursos propios del agente, ya sean públicas o privadas, que se facilite con el fin de mejorar la accesibilidad, no tendrán derecho a invocar la letra b) del apartado 1.

7. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 26 para completar el anexo VI, precisando en mayor medida los criterios pertinentes que deba tener en cuenta el agente económico para la evaluación a que se refiere el apartado 2 del presente artículo. Cuando precise en mayor medida dichos criterios, la Comisión tendrá en cuenta los beneficios potenciales no solo para las personas con discapacidad, sino también para las personas con limitaciones funcionales.

En caso necesario, la Comisión adoptará el primero de esos actos delegados a más tardar el 28 de junio de 2020. La aplicabilidad de dicho acto comenzará, como muy pronto, el 28 de junio de 2025.

8. Cuando los agentes económicos se acojan a lo dispuesto en el apartado 1 para un producto o servicio determinado remitirán información a tal fin a las correspondientes autoridades de vigilancia del mercado o a las autoridades responsables de verificar el cumplimiento de los servicios del Estado miembro en el que se introduce en el mercado el producto concreto o se preste el servicio concreto.

El párrafo primero no será aplicable a las microempresas.

CAPÍTULO VI

Normas armonizadas y especificaciones técnicas de los productos y servicios

Artículo 15

Presunción de conformidad

1. Se presumirá que los productos y servicios conformes con normas armonizadas o partes de estas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* cumplen los requisitos de accesibilidad establecidos en la presente Directiva, en la medida en que dichas normas o partes de ellas sean aplicables a dichos requisitos.

2. La Comisión solicitará, de conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, a uno o más organismos europeos de normalización que elaboren proyectos de normas armonizadas para los requisitos de accesibilidad de productos que figuran en el anexo I. La Comisión presentará el primer proyecto de solicitud de normas armonizadas al comité pertinente a más tardar el 28 de junio de 2021.

3. La Comisión podrá adoptar actos de ejecución que establezcan especificaciones técnicas que cumplan los requisitos de accesibilidad establecidos en la presente Directiva cuando se hayan cumplido las siguientes condiciones:

a) no se haya publicado ninguna referencia a normas armonizadas en el *Diario Oficial de la Unión Europea* de conformidad con el Reglamento (UE) n.º 1025/2012, y

b) bien:

   i) la Comisión haya solicitado a uno o más organismos europeos de normalización que elaboren normas armonizadas y se produzcan retrasos injustificados en el procedimiento de normalización o la solicitud no haya sido aceptada por ningún organismo europeo de normalización, bien

ii) la Comisión pueda demostrar que una especificación técnica respeta los requisitos establecidos en el anexo II del Reglamento (UE) n.º 1025/2012, excepto el requisito de que una organización sin ánimo de lucro haya elaborado las especificaciones técnicas.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 27, apartado 2.

4. Se presumirá que los productos y servicios conformes con las especificaciones técnicas o con partes de estas cumplen los requisitos de accesibilidad establecidos en la presente Directiva, en la medida en que dichas especificaciones técnicas o partes de ellas sean aplicables a dichos requisitos.

CAPÍTULO VII

Conformidad de los productos y marcado CE

Artículo 16

Declaración UE de conformidad de los productos

1. La declaración UE de conformidad confirmará que se ha demostrado el cumplimiento de los requisitos de accesibilidad aplicables. Cuando, como excepción, se haya utilizado el artículo 14, en la declaración UE de conformidad constarán los requisitos de accesibilidad que están sujetos a dicha excepción.

2. La declaración UE de conformidad se ajustará a la estructura del modelo establecido en el anexo III de la Decisión n.º 768/2008/CE. Contendrá los elementos especificados en el anexo IV de la presente Directiva y se mantendrá actualizada continuamente. Los requisitos relativos a la documentación técnica evitarán imponer una carga injustificada a las microempresas y las pymes. Se traducirá a la lengua o las lenguas que exija el Estado miembro en cuyo mercado se introduzca o se comercialice el producto.

3. Cuando un producto esté sujeto a más de un acto de la Unión que exija una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos esos actos de la Unión. Dicha declaración contendrá la identificación de los actos correspondientes, incluidas las referencias de publicación.

4. Al elaborar una declaración UE de conformidad, el fabricante asumirá la responsabilidad de la conformidad del producto con los requisitos establecidos en la presente Directiva.

Artículo 17

Principios generales del marcado CE de los productos

El marcado CE estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.

Artículo 18

Reglas y condiciones para la colocación del marcado CE

1. El marcado CE se colocará en el producto o su placa de datos de manera visible, legible e indeleble. Cuando esto no sea posible o no pueda garantizarse debido a la naturaleza del producto, se colocará en el embalaje o envase y en los documentos adjuntos.

2. El marcado CE se colocará antes de la introducción del producto en el mercado.

3. Los Estados miembros se basarán en los mecanismos existentes para garantizar la correcta aplicación del régimen que regula el marcado CE y emprenderán las acciones oportunas en caso de uso incorrecto de dicho marcado.

CAPÍTULO VIII

Vigilancia del mercado de los productos y procedimiento de salvaguardia de la Unión

Artículo 19

Vigilancia del mercado de los productos

1. Serán aplicables a los productos el artículo 15, apartado 3, los artículos 16 a 19, el artículo 21, los artículos 23 a 28 y el artículo 29, apartados 2 y 3, del Reglamento (CE) n.º 765/2008.

2. Cuando lleven a cabo la vigilancia del mercado de los productos, las autoridades de vigilancia del mercado pertinentes, cuando el agente económico se acoja al artículo 14 de la presente Directiva:

a) comprobarán que el agente económico ha llevado a cabo la evaluación a que se refiere el artículo 14;

b) examinarán dicha evaluación y sus resultados, en particular la correcta aplicación de los criterios que figuran en el anexo VI, y

c) comprobarán el cumplimiento de los requisitos de accesibilidad aplicables.

3. Los Estados miembros garantizarán que la información en poder de las autoridades de vigilancia del mercado sobre la conformidad de los agentes económicos con los requisitos de accesibilidad aplicables establecidos en la presente Directiva y la evaluación prevista en el artículo 14 se pongan a disposición de los consumidores, previa solicitud y en un formato accesible, excepto cuando dicha información no pueda facilitarse por motivos de confidencialidad con arreglo al artículo 19, apartado 5, del Reglamento (CE) n.º 765/2008.

Artículo 20

Procedimiento a escala nacional para los productos que no cumplen los requisitos de accesibilidad aplicables

1. Cuando las autoridades de vigilancia del mercado de un Estado miembro tengan motivos suficientes para pensar que un producto incluido en el ámbito de aplicación de la presente Directiva no cumple los requisitos de accesibilidad aplicables, efectuarán una evaluación del producto con respecto a todos los requisitos establecidos en la presente Directiva. Los agentes económicos correspondientes cooperarán plenamente a este fin con las autoridades de vigilancia del mercado.

Si, en el transcurso de la evaluación a que se refiere el párrafo primero, las autoridades de vigilancia del mercado constatan que el producto no cumple los requisitos establecidos en la presente Directiva, pedirán sin demora al agente económico en cuestión que adopte todas las medidas correctoras adecuadas para que el producto cumpla dichos requisitos en el plazo razonable, proporcional a la naturaleza del incumplimiento, que ellas prescriban.

Las autoridades de vigilancia del mercado exigirán al agente económico en cuestión que retire el producto del mercado en un plazo adicional razonable, únicamente si dicho agente económico no hubiera adoptado las medidas correctoras adecuadas en el plazo mencionado en el párrafo segundo.

El artículo 21 del Reglamento (CE) n.º 765/2008 será aplicable a las medidas mencionadas en los párrafos segundo y tercero del presente apartado.

2. Cuando las autoridades de vigilancia del mercado consideren que el incumplimiento no se limita al territorio nacional, informarán a la Comisión y a los demás Estados miembros de los resultados de la evaluación y de las medidas que hayan pedido al agente económico que adopte.

3. El agente económico se asegurará de que se adopten todas las medidas correctoras pertinentes en relación con todos los productos afectados que haya comercializado en toda la Unión.

4. Si el agente económico en cuestión no adoptara las medidas correctoras adecuadas en el plazo de tiempo indicado en el apartado 1, párrafo tercero, las autoridades de vigilancia del mercado adoptarán todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del producto en el mercado nacional o para retirarlo de él.

Las autoridades de vigilancia del mercado informarán sin demora a la Comisión y a los demás Estados miembros de tales medidas.

5. La información a que se refiere el apartado 4, párrafo segundo, incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del producto no conforme, el origen del producto, la naturaleza de la supuesta no conformidad y los requisitos de accesibilidad que el producto incumple, la naturaleza y duración de las medidas nacionales adoptadas, así como los argumentos expresados por el agente económico en cuestión. En particular, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno de los motivos siguientes:

a) el producto incumple los requisitos de accesibilidad aplicables, o

b) defectos en las normas armonizadas o en las especificaciones técnicas a que se refiere el artículo 15 que confieren la presunción de conformidad.

6. Los Estados miembros distintos de aquel que inició el procedimiento con arreglo al presente artículo informarán sin demora a la Comisión y a los demás Estados miembros de toda medida que adopten y de cualquier dato adicional sobre la no conformidad del producto en cuestión que tengan a su disposición y, en caso de desacuerdo con la medida nacional notificada, presentarán sus objeciones al respecto.

7. Si en el plazo de tres meses tras la recepción de la información a que se refiere el apartado 4, párrafo segundo, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por un Estado miembro, la medida se considerará justificada.

8. Los Estados miembros velarán por que se adopten sin demora las medidas restrictivas adecuadas respecto del producto en cuestión, tales como la retirada del producto de su mercado.

Artículo 21

Procedimiento de salvaguardia de la Unión

1. Si, una vez concluido el procedimiento establecido en el artículo 20, apartados 3 y 4, se formulan objeciones contra una medida adoptada por un Estado miembro o si la Comisión tiene pruebas razonables indiciarias de que una medida nacional vulnera el Derecho de la Unión, la Comisión consultará sin demora a los Estados miembros y al agente o los agentes económicos en cuestión y procederá a la evaluación de la medida nacional. Sobre la base de los resultados de esa evaluación, la Comisión decidirá si la medida nacional está justificada.

La Comisión comunicará inmediatamente su decisión a todos los Estados miembros y al agente o los agentes económicos en cuestión.

2. Si se considera justificada la medida nacional a que se refiere el apartado 1, todos los Estados miembros adoptarán las medidas necesarias para garantizar la retirada de su mercado del producto no conforme e informarán de ello a la Comisión. Si la medida nacional no se considera justificada, el Estado miembro en cuestión retirará la medida.

3. Si la medida nacional a que se refiere el apartado 1 del presente artículo se considera justificada y la no conformidad del producto se atribuye a defectos de las normas armonizadas a que hace referencia el artículo 20, apartado 5, letra b), la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n.º 1025/2012.

4. Si la medida nacional a que se refiere el apartado 1 del presente artículo se considera justificada y la no conformidad del producto se atribuye a defectos de las especificaciones técnicas a que hace referencia el artículo 20, apartado 5, letra b), la Comisión adoptará sin demora actos de ejecución que modifiquen o deroguen la especificación técnica de que se trate. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 27, apartado 2.

Artículo 22

Incumplimiento formal

1. Sin perjuicio de lo dispuesto en el artículo 20, si un Estado miembro constata una de las situaciones indicadas a continuación, pedirá al agente económico correspondiente que subsane la no conformidad en cuestión:

a) el marcado CE se haya colocado incumpliendo el artículo 30 del Reglamento (CE) n.º 765/2008 o el artículo 18 de la presente Directiva;

b) el marcado CE no se haya colocado;

c) la declaración UE de conformidad no se haya establecido;

d) la declaración UE de conformidad no se haya establecido correctamente;

e) la documentación técnica no esté disponible o esté incompleta;

f) la información a que se refiere el artículo 7, apartado 6, o el artículo 9, apartado 4, falte, sea falsa o esté incompleta;

g) no se haya cumplido algún otro requisito administrativo establecido en el artículo 7 o en el artículo 9.

2. Si la no conformidad a que se refiere el apartado 1 persiste, el Estado miembro en cuestión adoptará todas las medidas adecuadas para restringir o prohibir la comercialización del producto o para asegurarse de que sea retirado del mercado.

CAPÍTULO IX

Conformidad de los servicios

Artículo 23

Conformidad de los servicios

1. Los Estados miembros establecerán, aplicarán y actualizarán periódicamente procedimientos adecuados para:

a) comprobar la conformidad de los servicios con los requisitos de la presente Directiva, en particular la evaluación a que se refiere el artículo 14, respecto de la cual el artículo 19, apartado 2, se aplicará *mutatis mutandis*;

b) hacer un seguimiento de las quejas o los informes sobre no conformidad de los servicios con los requisitos de accesibilidad establecidos en la presente Directiva;

c) verificar que el agente económico haya adoptado las medidas correctoras necesarias.

2. Los Estados miembros designarán a las autoridades responsables de la ejecución de los procedimientos a que se refiere el apartado 1 en lo que respecta a la conformidad de los servicios.

Los Estados miembros garantizarán que se informa al público de la existencia, las responsabilidades, la identidad, la labor y las decisiones de las autoridades a que se refiere el párrafo primero. Cuando así se les solicite, dichas autoridades pondrán a disposición dicha información en formatos accesibles.

CAPÍTULO X

Requisitos de accesibilidad en otros actos de la Unión

Artículo 24

Accesibilidad en virtud de otros actos de la Unión

1. En lo que se refiere a los productos y servicios a que se refiere el artículo 2 de la presente Directiva, los requisitos de accesibilidad que figuran en el anexo I de la presente Directiva constituirán requisitos de accesibilidad de carácter imperativo con arreglo al artículo 42, apartado 1, de la Directiva 2014/24/UE y al artículo 60, apartado 1, de la Directiva 2014/25/UE.

2. Se presumirá que todo producto o servicio cuyas características, elementos o funciones sean conformes con los requisitos de accesibilidad que figuran en el anexo I de la presente Directiva, de conformidad con la sección VI de dicho anexo, cumple con las obligaciones establecidas en actos de la Unión distintos de la presente Directiva, en lo que respecta a la accesibilidad, respecto de dichas características, elementos o funciones, salvo que esos actos establezcan otra cosa.

Artículo 25

Normas armonizadas y especificaciones técnicas para otros actos de la Unión

La conformidad con las normas armonizadas y especificaciones técnicas adoptadas con arreglo al artículo 15, o parte de ellas, conllevará la presunción de conformidad con el artículo 24 en la medida en que dichas normas y especificaciones técnicas, o parte de ellas, se ajusten a los requisitos de accesibilidad establecidos en la presente Directiva.

CAPÍTULO XI

Actos delegados, competencias de ejecución y disposiciones finales

Artículo 26

Ejercicio de la delegación

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

2. Los poderes para adoptar actos delegados mencionados en el artículo 4, apartado 9, se otorgan a la Comisión por un período de tiempo indefinido a partir del 27 de junio de 2019.

Los poderes para adoptar actos delegados mencionados en el artículo 12, apartado 3, y el artículo 14, apartado 7, se otorgan a la Comisión por un período de cinco años a partir del 27 de junio de 2019. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 4, apartado 9, el artículo 12, apartado 3, y el artículo 14, apartado 7, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

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

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

6. Los actos delegados adoptados en virtud del artículo 4, apartado 9, del artículo 12, apartado 3, y del artículo 14, apartado 7, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 27

Procedimiento de comité

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

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 28

Grupo de trabajo

La Comisión constituirá un grupo de trabajo compuesto por representantes de las autoridades de vigilancia del mercado, las autoridades responsables de verificar la conformidad de los servicios y las partes interesadas pertinentes, incluidos representantes de organizaciones de personas con discapacidad.

El grupo de trabajo deberá:

a) facilitar el intercambio de información y mejores prácticas entre las autoridades y las partes interesadas pertinentes;

b) fomentar la cooperación entre las autoridades y las partes interesadas pertinentes en cuestiones relacionadas con la aplicación de la presente Directiva para mejorar la coherencia en la aplicación de los requisitos de accesibilidad que figuran en la presente Directiva y para supervisar estrechamente la aplicación del artículo 14, y

c) proporcionar asesoramiento, en particular a la Comisión, especialmente sobre la aplicación de los artículos 4 y 14.

Artículo 29

Vigilancia del cumplimiento

1. Los Estados miembros garantizarán que existan medios adecuados y eficaces para asegurar el cumplimiento de la presente Directiva.

2. Los medios a que se refiere el apartado 1 incluirán:

a) disposiciones en virtud de las cuales un consumidor pueda llevar a cabo actuaciones conforme al Derecho interno ante los tribunales o ante los organismos administrativos competentes para garantizar que se cumplen las disposiciones nacionales de transposición de la presente Directiva;

b) disposiciones en virtud de las cuales los organismos públicos o las asociaciones, organizaciones u otras entidades jurídicas de carácter privado que tengan un interés legítimo en garantizar el cumplimiento de la presente Directiva puedan actuar conforme al Derecho interno ante los tribunales o ante los organismos administrativos competentes bien en nombre del demandante, bien en su apoyo y con su autorización, en cualquier procedimiento judicial o administrativo previsto para exigir el cumplimiento de las obligaciones en virtud de la presente Directiva.

3. El presente artículo no será aplicable a los procedimientos de contratación pública sujetos a la Directiva 2014/24/UE o a la Directiva 2014/25/UE.

Artículo 30

Sanciones

1. Los Estados miembros establecerán el régimen de sanciones aplicables a cualquier infracción de las disposiciones nacionales adoptadas al amparo de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su ejecución.

2. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias. Dichas sanciones también irán acompañadas de medidas correctoras efectivas en caso de incumplimiento por parte de los agentes económicos.

3. Los Estados miembros notificarán a la Comisión sin demora el régimen establecido y las medidas adoptadas y le comunicarán sin demora toda modificación posterior.

4. Las sanciones tendrán en cuenta el alcance de la no conformidad, incluidos su gravedad y el número de unidades de los productos o servicios no conformes de que se trate, así como el número de personas afectadas.

5. El presente artículo no será aplicable a los procedimientos de contratación sujetos a la Directiva 2014/24/UE o a la Directiva 2014/25/UE.

Artículo 31

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar el 28 de junio de 2022, 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.

2. Aplicarán dichas disposiciones a partir del 28 de junio de 2025.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, los Estados miembros podrán decidir aplicar las disposiciones relativas a las obligaciones establecidas en el artículo 4, apartado 8, a más tardar a partir del 28 de junio de 2027.

4. Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una 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.

5. 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.

6. Los Estados miembros que hagan uso de la posibilidad prevista en el artículo 4, apartado 4, comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten a tal fin e informarán a la Comisión de los avances realizados en su aplicación.

Artículo 32

Medidas transitorias

1. Sin perjuicio del apartado 2 del presente artículo, los Estados miembros dispondrán de un período transitorio que finalizará el 28 de junio de 2030, durante el que los prestadores de servicios podrán seguir prestando sus servicios mediante los productos que habían estado utilizando legalmente para prestar servicios similares antes de dicha fecha.

Los contratos de servicios celebrados antes del 28 de junio de 2025 podrán continuar sin cambios hasta su expiración, pero sin superar una duración de cinco años a partir de dicha fecha.

2. Los Estados miembros podrán disponer la posibilidad de que los terminales de autoservicio utilizados legalmente por los prestadores de servicios para la prestación de servicios antes del 28 de junio de 2025 se sigan utilizando para la prestación de servicios similares hasta el final de su vida útil desde el punto de vista económico, aunque sin superar los veinte años después de su puesta en funcionamiento.

Artículo 33

Informe y revisión

1. A más tardar, el 28 de junio de 2030, y posteriormente cada cinco años, la Comisión presentará al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones un informe sobre la aplicación de la presente Directiva.

2. Los informes abordarán, entre otros elementos, a la luz de los avances sociales, económicos y tecnológicos, la evolución de la accesibilidad de los productos y servicios, el posible bloqueo tecnológico o las barreras a la innovación y las repercusiones de la presente Directiva en los agentes económicos y personas con discapacidad. Los informes evaluarán, asimismo, si la aplicación del artículo 4, apartado 4, ha contribuido a aproximar aquellos requisitos de accesibilidad que sean divergentes relativos al entorno construido de los servicios de transporte de viajeros, servicios bancarios para consumidores y centros de servicio al usuario de tiendas de prestadores de servicios de comunicaciones electrónicas, cuando sea posible, con el fin de permitir un ajuste progresivo de los requisitos de accesibilidad que figuran en el anexo III.

Asimismo, los informes evaluarán si la aplicación de la presente Directiva, en particular, de sus disposiciones de carácter facultativo, ha contribuido a aproximar los requisitos de accesibilidad de las obras que constituyen el entorno construido que entran en el ámbito de aplicación de la Directiva 2014/23/UE del Parlamento Europeo y del Consejo ([35]), la Directiva 2014/24/UE y la Directiva 2014/25/UE.

Los informes también abordarán los efectos que tenga en el funcionamiento del mercado interior la aplicación del artículo 14 de la presente Directiva, en particular sobre la base de la información recibida de conformidad con el artículo 14, apartado 8, cuando se disponga de ella, así como las exenciones aplicables a las microempresas. Los informes determinarán si la presente Directiva ha alcanzado sus objetivos y si sería adecuado incluir nuevos productos y servicios en su ámbito de aplicación, o excluir ciertos productos y servicios de dicho ámbito de aplicación, y determinarán, cuando sea posible, ámbitos para la reducción de la carga con miras a una posible revisión de la presente Directiva.

Si fuera necesario, la Comisión propondrá medidas adecuadas, que podrán incluir medidas legislativas.

([35]) Directiva 2014/23/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la adjudicación de contratos de concesión (DO L 94 de 28.3.2014, p. 1).

3. Los Estados miembros comunicarán a la Comisión puntualmente toda la información necesaria para que la Comisión elabore dichos informes.

4. Los informes de la Comisión tendrán en cuenta las opiniones de los agentes económicos y de las organizaciones no gubernamentales pertinentes, incluidas aquellas que representan a las personas con discapacidad.

Artículo 34

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

Artículo 35

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

ANEXO I

REQUISITOS DE ACCESIBILIDAD DE LOS PRODUCTOS Y SERVICIOS

Sección I

Requisitos generales de accesibilidad relacionados con todos los productos incluidos en el ámbito de aplicación de la presente Directiva de conformidad con el artículo 2, apartado 1

Los productos deberán diseñarse y fabricarse de tal manera que se optimice su uso previsible por parte de las personas con discapacidad y vayan acompañados, en la medida de lo posible, en el producto o sobre él, de información accesible sobre su funcionamiento y características de accesibilidad.

1. Requisitos relativos al suministro de información:

   a) la información sobre el uso del producto facilitada en el propio producto (etiquetado, instrucciones y advertencias):

      i) estará disponible a través de más de un canal sensorial,

      ii) se presentará de una forma fácil de entender,

      iii) se presentará a los usuarios de una forma que puedan percibir,

      iv) se presentará utilizando un tipo de letra de tamaño adecuado y forma conveniente, teniendo en cuenta las condiciones previsibles de uso, así como utilizando un contraste suficiente y un espaciado ajustable entre letra s), líneas y párrafos;

   b) las instrucciones de uso del producto, cuando no se proporcionen con el propio producto, sino a través del uso del producto o por otros medios, como un sitio web (por ejemplo las funciones de accesibilidad del producto, cómo activarlas y su interoperabilidad con soluciones de apoyo), se pondrán a disposición del público en el momento en que se introduzca en el mercado, y:

      i) estarán disponibles a través de más de un canal sensorial,

      ii) se presentarán de una forma que resulte fácil de entender,

      iii) se presentarán a los usuarios de una forma que puedan percibir,

      iv) se presentarán utilizando un tipo de letra de tamaño adecuado y forma conveniente, teniendo en cuenta las condiciones previsibles de uso, así como utilizando un contraste suficiente y un espaciado ajustable entre letra s), líneas y párrafos,

      v) con respecto al contenido, estarán disponibles en formatos de texto que puedan utilizarse para generar formatos de apoyo que puedan presentarse de diversas formas y a través de más de un canal sensorial,

      vi) irán acompañadas de una presentación alternativa del contenido no textual,

      vii) incluirán una descripción de la interfaz de usuario del producto (manipulación, control y respuesta, entrada y salida de datos) proporcionada de conformidad con el punto 2; la descripción indicará, para cada una de las letras contenidas en el punto 2, si el producto presenta dichas características,

      viii) incluirán una descripción de la funcionalidad del producto proporcionada por las funciones destinadas a satisfacer las necesidades de las personas con discapacidad, de conformidad con el punto 2; la descripción indicará, para cada una de las letras contenidas en el punto 2, si el producto presenta dichas características,

      ix) incluirán una descripción de la interconexión del programa y el aparato del producto con dispositivos de apoyo; la descripción incluirá una lista de las tecnologías de apoyo que se han ensayado junto con el producto.

2. Interfaz de usuario y diseño de funcionalidad:

   El producto, incluida su interfaz de usuario, contendrá características, elementos y funciones que permitan a las personas con discapacidad acceder, percibir, manejar, comprender y controlar el producto, velando por lo siguiente:

   a) cuando el producto proporcione las funciones de comunicación —incluida la comunicación interpersonal—, manejo, información, control y orientación, lo hará a través de más de un canal sensorial, lo que incluirá ofrecer alternativas a la comunicación visual, auditiva, hablada y táctil;

   b) cuando el producto utilice el habla, proporcionará alternativas al habla y a la intervención vocal para la comunicación, el manejo, el control y la orientación;

c) cuando el producto utilice elementos visuales, proporcionará funciones flexibles de aumento, brillo y contraste para la comunicación, la información y el manejo, y garantizará la interoperabilidad con los programas y las tecnologías de apoyo para navegar por la interfaz;

d) cuando el producto utilice el color para transmitir información, indicar una acción, pedir una respuesta o identificar elementos, proporcionará una alternativa al color;

e) cuando el producto utilice señales audibles para transmitir información, indicar una acción, pedir una respuesta o identificar elementos, proporcionará una alternativa a las señales audibles;

f) cuando el producto utilice elementos visuales, proporcionará formas flexibles de mejorar la claridad de visión;

g) cuando el producto utilice audio, proporcionará la posibilidad de que el usuario controle el volumen y la velocidad, y características de audio mejoradas, en particular la reducción de interferencias de señales de audio procedentes de los productos circundantes y la claridad del audio;

h) cuando el producto requiera un manejo y control manuales, proporcionará la posibilidad de un control secuencial y alternativas a la motricidad precisa, evitando la necesidad de controles simultáneos para la manipulación, y utilizará partes discernibles al tacto;

i) el producto evitará modos de manejo que exijan amplio alcance y mucha fuerza;

j) el producto evitará la activación de reacciones fotosensibles;

k) el producto protegerá la privacidad del usuario cuando este utilice características de accesibilidad;

l) el producto proporcionará una alternativa a la identificación y el control biométricos;

m) el producto garantizará la coherencia de la funcionalidad y proporcionará lapsos de tiempo suficientes y flexibles para la interacción;

n) el producto proporcionará el programa y el aparato para la interfaz con las tecnologías asistenciales;

o) el producto cumplirá los siguientes requisitos específicos del sector:

i) terminales de autoservicio:

— integrarán una tecnología de síntesis vocal,

— permitirán la utilización de auriculares,

— cuando el tiempo de respuesta sea limitado, avisarán al usuario a través de más de un canal sensorial,

— darán la posibilidad de aumentar el tiempo de respuesta,

— tendrán un contraste adecuado y, cuando dispongan de teclas y controles, estos serán perceptibles al tacto,

— no requerirán que esté activada una característica de accesibilidad para que un usuario que necesite dicha característica las encienda,

— cuando el producto utilice audio o señales acústicas, será compatible con los dispositivos y tecnología de apoyo disponibles a escala de la Unión, incluidas tecnologías auditivas, tales como audífonos, telebobinas, implantes cocleares y dispositivos de escucha asistida,

ii) los lectores electrónicos integrarán una tecnología de síntesis vocal,

iii) equipos terminales de consumo con capacidad informática interactiva utilizados para la prestación de servicios de comunicaciones electrónicas:

— cuando dichos productos tengan capacidad textual además de vocal, incluirán la posibilidad de manejo textual en tiempo real y ofrecerán un sonido de alta fidelidad,

— cuando tengan capacidad para utilizar vídeo, además de capacidad textual y vocal o combinada con estas últimas, deberán posibilitar el manejo de la conversación completa, incluida la voz sincronizada, el texto en tiempo real y el vídeo, con una resolución que permita la comunicación mediante el lenguaje de signos,

— garantizarán una conexión inalámbrica eficaz con las tecnologías auditivas,

— evitarán las interferencias con dispositivos de apoyo,

iv) los equipos terminales de consumo con capacidad de computación interactiva utilizados para acceder a servicios de comunicación audiovisual pondrán a disposición de las personas con discapacidad los componentes de accesibilidad proporcionados por el prestador de servicios de comunicación audiovisual, para el acceso, la selección, el control y la personalización del usuario y para la transmisión a dispositivos de apoyo.

3. Servicios de apoyo:

Cuando se disponga de ellos, los servicios de apoyo (puntos de contacto, centros de asistencia telefónica, asistencia técnica, servicios de retransmisión y servicios de formación) ofrecerán información sobre la accesibilidad del producto y su compatibilidad con las tecnologías asistenciales, en modos de comunicación accesibles para las personas con discapacidad.

Sección II

Requisitos de accesibilidad relacionados con los productos del artículo 2, apartado 1, excepto los terminales de autoservicio a que se refiere el artículo 2, apartado 1, letra b)

Además de los requisitos de la sección I, con el fin de optimizar su uso previsible por las personas con discapacidad, se harán accesibles los embalajes o envases e instrucciones de los productos incluidos en la presente sección. A saber:

a) el embalaje o envase del producto, en particular la información facilitada en él (por ejemplo, sobre la apertura, el cierre, el uso, la eliminación), incluido, cuando se disponga de ella, la información sobre sus características de accesibilidad, se hará accesible y, en la medida de lo posible, dicha información accesible figurará en el propio embalaje o envase;

b) las instrucciones de instalación y mantenimiento, almacenamiento y eliminación del producto no suministradas con el propio producto pero disponibles por otros medios, como, por ejemplo, un sitio web, se pondrán a disposición del público cuando el producto se introduzca en el mercado y deberán cumplir los requisitos siguientes:

i) estarán disponibles a través de más de un canal sensorial,

ii) se presentarán de una forma que resulte fácil de entender,

iii) se presentarán a los usuarios de una forma que puedan percibir,

iv) se presentarán en un tipo de letra de tamaño adecuado y forma conveniente, teniendo en cuenta las condiciones previsibles de uso, así como utilizando un contraste suficiente y un espaciado ajustable entre letra s), líneas y párrafos,

v) el contenido de las instrucciones estará disponible en formatos de texto que puedan utilizarse para generar formatos asistenciales alternativos para su presentación de diferentes modos y a través de más de un canal sensorial, y

vi) las instrucciones que contengan cualquier elemento de contenido no textual irán acompañadas de una presentación alternativa de dicho contenido.

Sección III

Requisitos generales de accesibilidad relacionados con todos los servicios incluidos en el ámbito de aplicación de la presente Directiva de conformidad con el artículo 2, apartado 2

Con el fin de optimizar su uso previsible por las personas con discapacidad, la prestación de los servicios se efectuará:

a) garantizando la accesibilidad de los productos usados para la prestación del servicio de conformidad con lo dispuesto en la sección I del presente anexo y, cuando proceda, en su sección II;

b) proporcionando información sobre el funcionamiento del servicio, y, cuando se utilicen productos para la prestación del servicio, su vinculación con dichos productos, así como información sobre sus características de accesibilidad e interoperabilidad con dispositivos y equipamientos de apoyo:

i) haciendo disponible la información a través de más de un canal sensorial,

ii) presentando la información de una forma que resulte fácil de entender,

iii) presentando la información a los usuarios de una forma que puedan percibir,

iv) velando por que el contenido de la información esté disponible en formatos de texto que puedan utilizarse para generar formatos asistenciales alternativos para su presentación de diferentes modos por los usuarios y a través de más de un canal sensorial,

v) presentándose en un tipo de letra de tamaño adecuado y forma conveniente, teniendo en cuenta las condiciones previsibles de uso, así como utilizando un contraste suficiente y un espaciado ajustable entre letra s), líneas y párrafos,

vi) complementando cualquier contenido con una presentación alternativa de dicho contenido, y

vii) ofreciendo la información electrónica necesaria para la prestación del servicio de manera coherente y adecuada, haciéndola perceptible, manejable, comprensible y sólida;

c) haciendo que los sitios web, incluidas las aplicaciones en línea conexas, y los servicios basados en dispositivos móviles, incluidas las aplicaciones para dispositivos móviles, sean accesibles de manera coherente y adecuada haciéndolos perceptibles, manejables, comprensibles y sólidos;

d) cuando se disponga de ellos, los servicios de apoyo (puntos de contacto, centros de asistencia telefónica, asistencia técnica, servicios de retransmisión y servicios de formación) que faciliten información sobre la accesibilidad del servicio y su compatibilidad con las tecnologías de apoyo mediante modos de comunicación accesibles.

Sección IV

Requisitos adicionales de accesibilidad relacionados con servicios específicos

La prestación de servicios con el fin de optimizar su uso previsible por personas con discapacidades se obtendrá incluyendo las siguientes funciones, prácticas, políticas, procedimientos y cambios en el funcionamiento del servicio con la finalidad de abordar las necesidades de las personas con discapacidades y garantizar la interoperabilidad con las tecnologías de apoyo:

a) Servicios de comunicaciones electrónicas, en particular las comunicaciones de emergencia a que se refiere el artículo 109, apartado 2, de la Directiva (UE) 2018/1972:

i) facilitando el texto en tiempo real además de comunicación de voz;

ii) facilitando la conversación completa con apoyo de vídeo además de la comunicación de voz;

iii) velando por que las comunicaciones de emergencia que utilicen servicios de voz y texto —incluidos los textos en tiempo real— estén sincronizadas y que, en caso de que se facilite vídeo, también estén sincronizadas como una conversación completa y sean transmitidas por el prestador de servicios de comunicaciones electrónicas al punto de respuesta de seguridad pública más adecuado.

b) Servicios que proporcionan acceso a los servicios de comunicación audiovisual:

i) facilitando guías electrónicas de programas que sean perceptibles, funcionales, comprensibles y resistentes y que proporcionen información sobre la disponibilidad de características de accesibilidad;

ii) garantizando que los componentes de accesibilidad (servicios de acceso) de los servicios de comunicación audiovisual, como subtítulos para sordos y deficientes auditivos, descripción de audio, subtítulos hablados e interpretación de lenguaje de señas, se transmitan en su totalidad con calidad suficiente para una visualización precisa y sincronizada que posibilite al usuario controlar su presentación y utilización.

c) Servicios de transporte aéreo de viajeros, de transporte de viajeros por autobús, por ferrocarril y por vías navegables, salvo los servicios de transporte urbanos y suburbanos y los servicios de transporte regionales:

i) garantizando que se facilita información sobre la accesibilidad de los vehículos, de las infraestructuras circundantes y del entorno construido, así como sobre la asistencia para personas con discapacidad;

ii) garantizando que se facilita información sobre los terminales inteligentes expendedores de billetes (reservas electrónicas, compra de billetes, etc.), información de viaje en tiempo real (horarios, información sobre perturbaciones del tráfico, servicios de enlace, conexiones con otros modos de transporte, etc.) e información sobre servicios adicionales (personal de las estaciones, ascensores fuera de servicio o servicios temporalmente indisponibles).

d) Servicios de transporte urbanos y suburbanos y servicios de transporte regionales: garantizando la accesibilidad de los terminales de autoservicio usados para la prestación del servicio de conformidad con lo dispuesto en la sección I del presente anexo.

e) Servicios bancarios para consumidores:

i) facilitando métodos de identificación, firmas electrónicas, seguridad y servicios de pago que sean perceptibles, funcionales, comprensibles y resistentes;

ii) garantizando que la información sea comprensible, sin rebasar un nivel de complejidad superior al nivel B2 (intermedio alto) del Marco Común Europeo de Referencia para las Lenguas.

f) Libros electrónicos:

i) garantizando que, cuando un libro electrónico contenga audio además de texto, proporcione texto y audio sincronizados;

ii) garantizando que los archivos del libro electrónico no impidan que la tecnología de apoyo funcione correctamente;

iii) garantizando el acceso a los contenidos, la navegación por el contenido de los archivos y un diseño que incluya una configuración dinámica y aporte estructura, flexibilidad y variedad a la presentación de los contenidos;

iv) permitiendo presentaciones de sustitución del contenido y de su interoperabilidad con diversas tecnologías de apoyo, de forma que sea perceptible, utilizable, comprensible y fiable;

v) haciendo que se puedan explorar mediante el suministro de información sobre sus características de accesibilidad a través de metadatos;

vi) garantizando que las medidas de gestión de derechos digitales no bloqueen las características de accesibilidad.

g) Servicios de comercio electrónico:

i) facilitando la información relativa a la accesibilidad de los productos y servicios en venta cuando el agente económico responsable proporcione esta información;

ii) garantizando la accesibilidad de la función de identificación, seguridad y pago cuando se preste como parte de un servicio en lugar de un producto haciéndola perceptible, funcional, comprensible y resistente;

iii) facilitando métodos de identificación, firmas electrónicas y servicios de pago que sean perceptibles, funcionales, comprensibles y resistentes.

Sección V

Requisitos específicos de accesibilidad relacionados con la respuesta a las comunicaciones de emergencia al número único europeo de emergencia «112» por el punto de respuesta de seguridad pública (PSAP) más apropiado

Con el fin de optimizar su uso previsible por las personas con discapacidad, la respuesta a comunicaciones de emergencia al número único europeo de emergencia «112» por el PSAP más apropiado se realizará incluyendo funciones, prácticas, políticas, procedimientos y cambios destinados a atender a las necesidades de las personas con discapacidad.

Las comunicaciones de emergencia al número único europeo de emergencia «112» se responderán adecuadamente, de la manera que mejor convenga a la organización nacional de los sistemas de emergencia, por el PSAP más apropiado utilizando el mismo medio de comunicación que para su recepción, concretamente utilizando voz y texto sincronizados (en particular texto en tiempo real) o, si se facilita vídeo, voz, texto (en particular texto en tiempo real) y vídeo sincronizados como una conversación completa.

Sección VI

Requisitos de accesibilidad para características, elementos o funciones de los productos y servicios de conformidad con el artículo 24, apartado 2

La presunción de cumplimiento de las obligaciones pertinentes establecidas en otros actos de la Unión respecto de las características, elementos o funciones de los productos o servicios requiere lo siguiente:

1. Productos:

a) la accesibilidad de la información relativa al funcionamiento y a las características de accesibilidad relacionadas con los productos cumple los elementos correspondientes que figuran en la sección I, punto 1, del presente anexo, concretamente la información sobre la utilización del producto suministrada con el propio producto y las instrucciones de uso del producto, no facilitadas con el propio producto pero disponibles mediante la utilización del producto o por otros medios, como un sitio web;

b) la accesibilidad de las características, elementos y funciones de la interfaz de usuario y el diseño de funcionalidad de los productos cumple los correspondientes requisitos de accesibilidad, relativos a dicha interfaz de usuario o diseño de funcionalidad, establecidos en la sección I, punto 2, del presente anexo;

c) la accesibilidad del embalaje o envase, en particular la información que se suministra en él y las instrucciones de instalación y mantenimiento, almacenamiento y eliminación del producto no suministradas con el propio producto pero disponibles por otros medios, como por ejemplo un sitio web, salvo para los terminales de autoservicio, cumple los correspondientes requisitos de accesibilidad establecidos en la sección II del presente anexo.

2. Servicios:

La accesibilidad de las características, elementos y funciones de los servicios cumple los correspondientes requisitos de accesibilidad respecto de dichas características, elementos y funciones establecidos en las secciones del presente anexo relacionadas con los servicios.

Sección VII

Criterios de rendimiento funcional

Con el fin de optimizar su uso previsible por las personas con discapacidad, cuando los requisitos de accesibilidad que figuran en las secciones I a VI del presente anexo no aborden una o más funciones del diseño y fabricación de los productos o de la prestación de los servicios, dichas funciones o medios se harán accesibles mediante el cumplimiento de los criterios de rendimiento funcional correspondientes a los mismos.

Dichos criterios de rendimiento funcional solo podrán aplicarse como alternativa a uno o varios requisitos técnicos específicos cuando se haga referencia a ellos en los requisitos de accesibilidad, y ello exclusivamente en caso de que la aplicación de los pertinentes criterios de rendimiento funcional cumpla con los requisitos de accesibilidad y determine que el diseño y fabricación de los productos y la prestación de los servicios dan lugar a una accesibilidad equivalente o superior en el marco de una utilización previsible por personas con discapacidad.

a) Uso sin visión

Cuando el producto o servicio presente modos de utilización visuales, incluirá como mínimo un modo de utilización que no requiera visión.

b) Uso con visión limitada

Cuando el producto o servicio presente modos de utilización visuales, incluirá como mínimo un modo de utilización que permita a los usuarios servirse del producto con una visión limitada.

c) Uso sin percepción de color

Cuando el producto o servicio presente modos de utilización visuales, incluirá como mínimo un modo de utilización que no requiera la percepción del color por parte del usuario.

d) Uso sin audición

Cuando el producto o servicio presente modos de utilización auditivos, incluirá como mínimo un modo de utilización que no requiera audición.

e) Uso con audición limitada

Cuando el producto o servicio presente modos de utilización auditivos, incluirá como mínimo un modo de utilización con características de sonido mejoradas que permitan a los usuarios con audición limitada utilizar el producto.

f) Uso sin capacidad vocal

Cuando el producto o servicio requiera la intervención vocal de los usuarios, incluirá como mínimo un modo de utilización que no requiera una intervención vocal. La intervención vocal incluye cualesquiera sonidos generados de forma oral, como el habla, silbidos o chasquidos.

g) Uso con manipulación o esfuerzo limitados

Cuando el producto o servicio requiera acciones manuales, incluirá como mínimo un modo de utilización que permita a los usuarios manejarlo con ayuda de acciones alternativas que no requieran una manipulación o motricidad precisas, fuerza manual o el accionamiento simultáneo de más de un control.

h) Uso con alcance limitado

Los elementos operativos de los productos estarán al alcance de todos los usuarios. Cuando los productos o servicios presenten un modo manual de utilización, este incluirá como mínimo un modo de utilización que permita utilizarlos con una amplitud de movimientos y una fuerza limitadas.

i) Minimización del riesgo de activación de reacciones fotosensibles

Cuando el producto presente modos de utilización visuales, evitará los modos de utilización que desencadenen crisis fotosensibles.

j) Uso con conocimiento limitado

El producto o servicio ofrecerá como mínimo un modo de utilización que incorpore características que simplifiquen y faciliten su uso.

k) Privacidad

Cuando el producto o servicio presente características que permitan la accesibilidad, incluirá como mínimo un modo de utilización que mantenga la privacidad cuando se haga uso de dichas características.

ANEXO II

EJEMPLOS INDICATIVOS NO VINCULANTES DE POSIBLES SOLUCIONES QUE CONTRIBUYEN A CUMPLIR LOS REQUISITOS DE ACCESIBILIDAD QUE FIGURAN EN EL ANEXO I

SECCIÓN I:

EJEMPLOS RELACIONADOS CON LOS REQUISITOS GENERALES DE ACCESIBILIDAD DE TODOS LOS PRODUCTOS INCLUIDOS EN EL ÁMBITO DE APLICACIÓN DE LA PRESENTE DIRECTIVA DE CONFORMIDAD CON EL ARTÍCULO 2, APARTADO 1

REQUISITOS DE LA SECCIÓN I DEL ANEXO I	EJEMPLOS
1. Suministro de información	
a)	
i)	Proporcionando información visual y táctil o información visual y auditiva en el lugar en el que debe insertarse la tarjeta en un terminal de autoservicio, de manera que los ciegos y los sordos puedan hacer uso del terminal.
ii)	Empleando las mismas palabras de forma sistemática o con una estructura clara y lógica, de manera que las personas con discapacidad intelectual puedan entenderlas mejor.
iii)	Proporcionando un formato con relieve táctil o un sonido además de una advertencia de texto, de manera que las personas ciegas puedan percibirla.
iv)	Facilitando que el texto pueda ser leído por personas con discapacidad visual.
b)	
i)	Proporcionando archivos electrónicos que puedan ser leídos por ordenadores mediante el uso de lectores de pantalla, de manera que las personas ciegas puedan hacer uso de la información.
ii)	Empleando las mismas palabras de forma sistemática o con una estructura clara y lógica, de manera que las personas con discapacidad intelectual puedan entenderlas mejor.
iii)	Incluyendo subtítulos cuando se proporcionen instrucciones en vídeo.
iv)	Facilitando que el texto pueda ser leído por personas con discapacidad visual.
v)	Imprimiendo en Braille, de manera que una persona ciega pueda usar la información.
vi)	Acompañando un diagrama con un texto descriptivo que defina los elementos principales o describa las acciones clave.
vii)	No se aporta ejemplo.
viii)	No se aporta ejemplo.
ix)	Incluyendo en un cajero automático una toma de conexión y un programa informático que permita enchufar un auricular que reciba el texto mostrado en la pantalla en forma de sonido.

2. Interfaz de usuario y diseño de funcionalidad	
a)	Facilitando instrucciones en forma de voz y de texto, o incorporando señales táctiles en un teclado, de forma que las personas ciegas o con discapacidad auditiva puedan interactuar con el producto.
b)	Ofreciendo en un terminal de autoservicio además de instrucciones orales por ejemplo instrucciones en forma de texto o imágenes, de manera que una persona sorda pueda realizar también la acción requerida.
c)	Permitiendo a los usuarios ampliar el texto, enfocar en primer plano un pictograma particular o aumentar el contraste, de manera que las personas con discapacidad visual puedan percibir la información.
d)	Además de dar a elegir entre pulsar el botón verde o el rojo para seleccionar una opción, escribiendo las opciones sobre los botones para permitir a las personas daltónicas elegir la opción deseada.
e)	Cuando un ordenador emite una señal de error, mostrando un texto escrito o una imagen que indique el error para que las personas sordas puedan percibir que se está produciendo un error.
f)	Permitiendo aumentar el contraste en las imágenes en primer plano, de forma que las personas con baja visión puedan verlas.
g)	Permitiendo al usuario de un teléfono seleccionar el volumen del sonido y reducir las interferencias con las prótesis auditivas, de forma que las personas con discapacidad auditiva puedan usar el teléfono.
h)	Haciendo más grandes y separando bien los botones de las pantallas táctiles, de forma que las personas con temblores puedan pulsarlos.
i)	Velando por que los botones que se deban pulsar no requieran mucha fuerza, de modo que las personas con incapacidad motora puedan usarlos.
j)	Evitando las imágenes parpadeantes, de forma que las personas que sufren ataques epilépticos no corran riesgos.
k)	Permitiendo el uso de auriculares cuando se ofrece información oral en un cajero automático.
l)	Como alternativa al reconocimiento por huellas dactilares, permitiendo a los usuarios que no puedan hacer uso de sus manos elegir una contraseña para bloquear o desbloquear un teléfono.
m)	Velando por que el programa informático reaccione de manera predecible cuando se realiza una acción particular y dando tiempo suficiente para introducir una contraseña de manera que resulte fácil de utilizar para personas con discapacidad intelectual.
n)	Ofreciendo una conexión con una pantalla Braille, de forma que las personas ciegas puedan hacer uso del ordenador.
o)	Ejemplos de requisitos específicos del sector
i)	No se aporta ejemplo.
ii)	No se aporta ejemplo.
iii) Primer guion	Facilitando que un teléfono móvil pueda gestionar conversaciones en tiempo real, de forma que las personas con problemas auditivos puedan intercambiar información de manera interactiva.
iii) Cuarto guion	Permitiendo el uso simultáneo del vídeo para mostrar lengua de signos y texto para escribir un mensaje, de manera que dos personas sordas puedan comunicarse entre sí o con otra persona sin problemas auditivos.

iv)	Velando por que los subtítulos se transmitan a través del módulo de conexión para su uso por personas sordas.

3. Servicios de apoyo: No se aporta ejemplo.

SECCIÓN II:

EJEMPLOS RELACIONADOS CON LOS REQUISITOS DE ACCESIBILIDAD DE LOS PRODUCTOS DEL ARTÍCULO 2, APARTADO 1, EXCEPTO LOS TERMINALES DE AUTOSERVICIO A QUE SE REFIERE EL ARTÍCULO 2, APARTADO 1, LETRA b)

REQUISITOS DE LA SECCIÓN II DEL ANEXO I	EJEMPLOS
Embalajes o envases e instrucciones de los productos	
a)	Indicando en el embalaje que el teléfono incluye características de accesibilidad para personas con discapacidad.
b)	
i)	Proporcionando archivos electrónicos que puedan ser leídos por ordenadores mediante el uso de lectores de pantalla, de manera que las personas ciegas puedan hacer uso de la información.
ii)	Empleando las mismas palabras de forma sistemática o con una estructura clara y lógica, de manera que las personas con discapacidad intelectual puedan entenderlas mejor.
iii)	Proporcionando un formato con relieve táctil o un sonido cuando se muestre una advertencia en el texto, de manera que las personas ciegas puedan apreciar la advertencia.
iv)	Facilitando que el texto pueda ser leído por personas con discapacidad visual.
v)	Imprimiendo en Braille, de manera que una persona ciega pueda leerlo.
vi)	Complementando un diagrama con un texto descriptivo que defina los elementos principales o describa las acciones clave.

SECCIÓN III:

EJEMPLOS RELACIONADOS CON LOS REQUISITOS GENERALES DE ACCESIBILIDAD PARA TODOS LOS SERVICIOS INCLUIDOS EN EL ÁMBITO DE APLICACIÓN DE LA PRESENTE DIRECTIVA DE CONFORMIDAD CON EL ARTÍCULO 2, APARTADO 2

REQUISITOS DE LA SECCIÓN III DEL ANEXO I	EJEMPLOS
Prestación de servicios	
a)	No se aporta ejemplo.
b)	
i)	Proporcionando archivos electrónicos que puedan ser leídos por ordenadores mediante el uso de lectores de pantalla, de manera que las personas ciegas puedan hacer uso de la información.
ii)	Empleando las mismas palabras de forma sistemática o con una estructura clara y lógica, de manera que las personas con discapacidad intelectual puedan entenderlas mejor.
iii)	Proporcionando subtítulos cuando se presenta un vídeo con instrucciones.

iv)	Facilitando que una persona ciega pueda hacer uso de un archivo imprimiendo en Braille.
v)	Facilitando que el texto pueda ser leído por personas con discapacidad visual.
vi)	Complementando un diagrama con un texto descriptivo que defina los elementos principales o describa las acciones clave.
vii)	Cuando un prestador de servicios ofrezca una llave USB con información sobre el servicio, facilitando que esta información sea accesible.
c)	Proporcionando un texto descriptivo de las imágenes, haciendo que todas las funcionalidades estén disponibles desde un teclado, proporcionando a los usuarios tiempo suficiente para leer, haciendo que el contenido se muestre y opere de forma predecible o proporcionando compatibilidad con tecnologías de apoyo, de manera que personas con discapacidades diversas puedan leer e interactuar con un sitio web.
d)	No se aporta ejemplo.

SECCIÓN IV:

EJEMPLOS RELACIONADOS CON LOS REQUISITOS ADICIONALES DE ACCESIBILIDAD DE SERVICIOS ESPECÍFICOS

REQUISITOS DE LA SECCIÓN IV DEL ANEXO I	EJEMPLOS
Servicios específicos	
a)	
i)	Facilitando que las personas con problemas auditivos puedan escribir y recibir texto de forma interactiva y en tiempo real.
ii)	Facilitando que las personas sordas puedan utilizar la lengua de signos para comunicarse entre ellos.
iii)	Facilitando que una persona con discapacidad de habla y auditiva que opta por utilizar una combinación de texto, voz y vídeo sepa que la comunicación es transmitida a través de la red a un servicio de emergencia.
b)	
i)	Facilitando que una persona ciega pueda seleccionar programas en la televisión.
ii)	Ofreciendo la posibilidad de seleccionar, personalizar y visualizar «servicios de acceso», como subtítulos para personas sordas o con problemas auditivos, descripción de audio, subtítulos hablados e interpretación de lengua de signos, ofreciendo medios que permitan una conexión inalámbrica eficaz con las tecnologías auditivas o bien poniendo a disposición de los usuarios los controles necesarios para activar «servicios de acceso» a servicios de comunicación audiovisual con el mismo grado de importancia que los controles de medios primarios.
c)	
i)	No se aporta ejemplo.
ii)	No se aporta ejemplo.
d)	No se aporta ejemplo.
e)	
i)	Velando por que los diálogos de identificación en pantalla sean legibles mediante el uso de lectores de pantalla, de forma que las personas ciegas puedan usarlos.

ii)	No se aporta ejemplo.
f)	
i)	Facilitando que una persona con dislexia pueda leer y escuchar el texto al mismo tiempo.
ii)	Habilitando la salida sincronizada del texto y el audio o una transcripción en una pantalla Braille.
iii)	Facilitando que una persona ciega pueda acceder al índice o cambiar de capítulo.
iv)	No se aporta ejemplo.
v)	Garantizando que la información sobre sus características de accesibilidad esté disponible en el archivo electrónico, de manera que las personas con discapacidad puedan estar informadas.
vi)	Asegurándose de que no se bloquee, por ejemplo, de que las medidas de protección técnica, la información sobre gestión de derechos o las cuestiones de interoperabilidad no impidan que el texto pueda ser leído en voz alta por dispositivos de apoyo, de forma que los usuarios ciegos puedan leer el libro.
g)	
i)	Asegurándose de que la información disponible sobre las características de accesibilidad de un producto no se suprima.
ii)	Haciendo que la interfaz de usuario del servicio de pago esté disponible por voz, de forma que las personas ciegas puedan hacer compras en línea de forma autónoma.
iii)	Velando por que los diálogos de identificación en pantalla sean legibles mediante el uso de lectores de pantalla, de forma que las personas ciegas puedan usarlos.

ANEXO III

REQUISITOS DE ACCESIBILIDAD A EFECTOS DEL ARTÍCULO 4, APARTADO 4, RELATIVOS AL ENTORNO FÍSICO DONDE SE PRESTAN LOS SERVICIOS INCLUIDOS EN EL ÁMBITO DE APLICACIÓN DE LA PRESENTE DIRECTIVA

Con el fin de optimizar el uso previsible de manera autónoma por las personas con discapacidad del entorno físico donde se presta el servicio y que recae bajo la responsabilidad del prestador de servicios, tal como dispone el artículo 4, apartado 4, la accesibilidad de las zonas destinadas al acceso público incluirá los siguientes aspectos:

a) uso de zonas e instalaciones al aire libre asociadas;

b) accesos a los edificios;

c) uso de entradas;

d) uso de vías de circulación horizontal;

e) uso de vías de circulación vertical;

f) uso de las salas por el público;

g) uso de equipos e instalaciones utilizados en la prestación del servicio;

h) uso de los aseos e instalaciones sanitarias;

i) uso de salidas, vías de evacuación y conceptos de planificación de emergencia;

j) comunicación y orientación a través de más de un canal sensorial;

k) uso de instalaciones y edificios para su finalidad previsible;

l) protección frente a peligros en el entorno interior y exterior.

ANEXO IV

PROCEDIMIENTO DE EVALUACIÓN DE LA CONFORMIDAD DE LOS PRODUCTOS

1. Control interno de la producción

El control interno de la producción es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2, 3 y 4 del presente anexo, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos en cuestión satisfacen los requisitos correspondientes de la presente Directiva.

2. Documentación técnica

El fabricante elaborará la documentación técnica. La documentación técnica permitirá evaluar si el producto cumple los requisitos de accesibilidad pertinentes contemplados en el artículo 4 y, en caso de que el fabricante se acoja al artículo 14, demostrar que los requisitos de accesibilidad pertinentes introducirían una modificación sustancial o impondrían una carga desproporcionada. La documentación técnica especificará únicamente los requisitos aplicables y contemplará, en la medida en que sea pertinente para la evaluación, el diseño, la fabricación y el funcionamiento del producto.

La documentación técnica incluirá, cuando proceda, al menos los siguientes elementos:

a) una descripción general del producto;

b) una lista de las normas armonizadas y especificaciones técnicas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, aplicadas íntegramente o en parte, así como descripciones de las soluciones adoptadas para cumplir los requisitos pertinentes de accesibilidad contemplados en el artículo 4, en caso de que no se hayan aplicado dichas normas armonizadas o especificaciones técnicas; en caso de normas armonizadas o especificaciones técnicas que se apliquen parcialmente, se especificarán en la documentación técnica las partes que se hayan aplicado.

3. Fabricación

El fabricante tomará todas las medidas necesarias para que el proceso de fabricación y su supervisión garanticen la conformidad de los productos con la documentación técnica mencionada en el punto 2 del presente anexo y con los requisitos de accesibilidad establecidos en la presente Directiva.

4. Marcado CE y declaración UE de conformidad

4.1. El fabricante colocará el marcado CE contemplado en la presente Directiva en cada producto individual que satisfaga los requisitos aplicables de la presente Directiva.

4.2. El fabricante redactará una declaración UE de conformidad para cada modelo de producto. En la declaración UE de conformidad se identificará el producto para el cual ha sido elaborada.

Se facilitará una copia de la declaración UE de conformidad a las autoridades competentes que lo soliciten.

5. Representante autorizado

Las obligaciones del fabricante mencionadas en el punto 4 podrá cumplirlas su representante autorizado, en su nombre y bajo su responsabilidad, siempre que estén especificadas en su mandato.

ANEXO V

INFORMACIÓN SOBRE LOS SERVICIOS QUE CUMPLEN LOS REQUISITOS DE ACCESIBILIDAD

1. El prestador del servicio incluirá en las condiciones generales, o un documento equivalente, la información que evalúe de qué manera el servicio cumple los requisitos de accesibilidad a que se refiere el artículo 4. La información describirá los requisitos aplicables y contemplará el diseño y el funcionamiento del servicio, en la medida en que sea pertinente para la evaluación. Además de los requisitos de información al consumidor de la Directiva 2011/83/UE, la información incluirá, cuando proceda, al menos los siguientes elementos:

   a) una descripción general del servicio en formatos accesibles;

   b) las descripciones y explicaciones necesarias para la comprensión del funcionamiento del servicio;

   c) una descripción de la forma en que el servicio cumple los requisitos de accesibilidad pertinentes establecidos en el anexo I.

2. Para cumplir el punto 1 del presente anexo, el prestador del servicio podrá aplicar, total o parcialmente, las normas armonizadas y especificaciones técnicas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*.

3. El prestador del servicio proporcionará información que demuestre que el proceso de prestación del servicio y su seguimiento garantizan la conformidad del servicio con el punto 1 del presente anexo y con los requisitos aplicables de la presente Directiva.

ANEXO VI

CRITERIOS PARA LA EVALUACIÓN DE LA CARGA DESPROPORCIONADA

Criterios para efectuar y documentar la evaluación:

1. La proporción de los costes netos de cumplir los requisitos de accesibilidad en los costes totales (inversiones en activos fijos y gastos operativos) de fabricar, distribuir o importar el producto o prestar el servicio para los agentes económicos.

   Elementos que han de emplearse para evaluar los costes netos de cumplir los requisitos de accesibilidad:

   a) criterios relacionados con costes organizativos puntuales que se deben tener en cuenta en la evaluación:

      i) costes relacionados con recursos humanos adicionales con experiencia en accesibilidad,

      ii) costes relacionados con la formación de los recursos humanos y la adquisición de competencias en materia de accesibilidad,

      iii) costes del desarrollo de un nuevo proceso para incluir la accesibilidad en el desarrollo del producto o la prestación del servicio,

      iv) costes relacionados con el desarrollo de material orientativo en materia de accesibilidad,

      v) costes puntuales para comprender la legislación sobre accesibilidad;

   b) criterios relacionados con la producción en curso y los costes de desarrollo que se deben tener en cuenta en la evaluación:

      i) costes relacionados con el diseño de las características de accesibilidad del producto o servicio,

      ii) costes soportados en los procesos de fabricación,

      iii) costes relacionados con los ensayos de los productos o servicios en lo que respecta a la accesibilidad,

      iv) costes relacionados con la elaboración de documentación.

2. Los costes y beneficios estimados para los agentes económicos, incluidos los procesos de producción y las inversiones, en relación con el beneficio estimado para las personas con discapacidad, teniendo en cuenta la cantidad y frecuencia de utilización de un producto o servicio específico.

3. La proporción de los costes netos de cumplir los requisitos de accesibilidad en el volumen de negocios neto del agente económico.

   Elementos que han de emplearse para evaluar los costes netos de cumplir los requisitos de accesibilidad:

   a) criterios relacionados con costes organizativos puntuales que se deben tener en cuenta en la evaluación:

      i) costes relacionados con recursos humanos adicionales con experiencia en accesibilidad,

      ii) costes relacionados con la formación de los recursos humanos y la adquisición de competencias en materia de accesibilidad,

      iii) costes del desarrollo de un nuevo proceso para incluir la accesibilidad en el desarrollo del producto o la prestación del servicio,

      iv) costes relacionados con el desarrollo de material orientativo en materia de accesibilidad,

      v) costes puntuales para comprender la legislación sobre accesibilidad;

   b) criterios relacionados con la producción en curso y los costes de desarrollo que se deben tener en cuenta en la evaluación:

      i) costes relacionados con el diseño de las características de accesibilidad del producto o servicio,

      ii) costes soportados en los procesos de fabricación,

      iii) costes relacionados con los ensayos de los productos o servicios en lo que respecta a la accesibilidad,

      iv) costes relacionados con la elaboración de documentación.

DIRECTIVA (UE) 2019/883 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

relativa a las instalaciones portuarias receptoras a efectos de la entrega de desechos generados por buques, por la que se modifica la Directiva 2010/65/UE y se deroga la Directiva 2000/59/CE

(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 100, apartado 2,

Vista la propuesta de la Comisión Europea,

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

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

Visto el dictamen del Comité de las Regiones ([2]),

De conformidad con el procedimiento legislativo ordinario ([3]),

Considerando lo siguiente:

(1) La política marítima de la Unión tiene por objetivo garantizar un elevado nivel de seguridad y de protección del medio ambiente. Ese objetivo puede lograrse mediante el cumplimiento de convenios, códigos y resoluciones internacionales, al tiempo que se conserva la libertad de navegación de conformidad con lo dispuesto en la Convención de las Naciones Unidas sobre el Derecho del Mar (CNUDM).

(2) El objetivo de desarrollo sostenible n.º 14 de las Naciones Unidas llama la atención sobre la amenaza que constituyen la contaminación marina y la contaminación por nutrientes, el agotamiento de los recursos y el cambio climático, fenómenos todos debidos principalmente a la acción humana. Estas amenazas aumentan la presión que sufren los ecosistemas, como la biodiversidad y la infraestructura natural, al tiempo que generan problemas socioeconómicos a escala mundial, en particular riesgos para la salud, la seguridad y la economía. La Unión debe actuar para proteger las especies marinas y apoyar a las personas que dependen de los océanos, ya sea para mantener su trabajo, para obtener recursos o para disfrutar de su tiempo libre.

(3) El Convenio internacional para prevenir la contaminación por los buques (Convenio MARPOL) establece prohibiciones generales para las descargas de los buques en el mar, pero también regula las condiciones en las cuales pueden descargarse determinados tipos de desechos en el medio marino. El Convenio MARPOL exige a las Partes Contratantes que garanticen la disponibilidad de instalaciones receptoras en los puertos.

(4) La Unión ha perseguido la aplicación de partes del Convenio MARPOL con la Directiva 2000/59/CE del Parlamento Europeo y del Consejo ([4]), aplicando un enfoque basado en los puertos. La Directiva 2000/59/CE pretende conciliar los intereses del buen funcionamiento del transporte marítimo con la protección del medio marino.

(5) En las dos últimas décadas, el Convenio MARPOL y sus anexos han sido objeto de importantes enmiendas, las cuales han ido fijando normas y prohibiciones más estrictas en relación con las descargas de desechos en el mar por parte de los buques.

(6) El anexo VI del Convenio MARPOL introdujo un conjunto de normas sobre descargas para nuevas categorías de desechos, en particular los residuos de los sistemas de limpieza de los gases de escape, que comprenden los lodos y el agua de purga de tales sistemas. Esas categorías de desechos deben incluirse en el ámbito de aplicación de la presente Directiva.

([1]) DO C 283 de 10.8.2018, p. 61.
([2]) DO C 461 de 21.12.2018, p. 220.
([3]) Posición del Parlamento Europeo de 13 de marzo de 2019 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.
([4]) Directiva 2000/59/CE del Parlamento Europeo y del Consejo, de 27 de noviembre de 2000, sobre instalaciones portuarias receptoras de desechos generados por buques y residuos de carga (DO L 332 de 28.12.2000, p. 81).

(7) Los Estados miembros deben seguir trabajando en el seno de la Organización Marítima Internacional (OMI) para que se tenga en cuenta de manera global el impacto medioambiental que tiene el vertido de aguas residuales procedentes de depuradoras en circuito abierto, incluidas medidas para contrarrestar posibles impactos.

(8) Debe animarse a los Estados miembros a tomar las medidas adecuadas conforme a lo dispuesto en la Directiva 2000/60/CE del Parlamento Europeo y del Consejo ([5]), en particular a prohibir el vertido de aguas residuales procedentes de depuradoras en circuito abierto y de determinados residuos de carga en sus aguas territoriales.

(9) El 1 de marzo de 2018, la OMI adoptó la versión revisada de las Orientaciones refundidas para los proveedores y usuarios de las instalaciones portuarias receptoras (MEPC.1/Circ.834/Rev.1) (en lo sucesivo, «Orientaciones refundidas de la OMI»), que contienen un formato normalizado del impreso de notificación previa para la entrega de desechos, un formato normalizado del recibo de entrega de desechos y para notificar supuestas deficiencias de las instalaciones portuarias receptoras, así como unas prescripciones de notificación en relación con las instalaciones receptoras de desechos.

(10) A pesar de esta evolución legislativa, siguen produciéndose descargas de desechos en el mar, con un importante coste medioambiental, social y económico. La persistencia de esas descargas se debe a una combinación de factores, a saber: en los puertos no siempre se dispone de instalaciones portuarias receptoras adecuadas, el control es con frecuencia insuficiente y no existen incentivos para entregar los desechos en tierra.

(11) La Directiva 2000/59/CE ha contribuido al incremento del volumen de desechos entregados a las instalaciones portuarias receptoras, entre otras maneras garantizando que los buques participan en los costes de dichas instalaciones, con independencia de su uso real de dichas instalaciones, por lo que ha sido esencial para reducir el vertido de desechos en el mar, tal como pone de manifiesto la evaluación de dicha Directiva llevada a cabo en el marco del programa de adecuación y eficacia de la reglamentación (en lo sucesivo, «evaluación REFIT»).

(12) La evaluación REFIT ha demostrado también que las incoherencias con el marco regulador del Convenio MARPOL han mermado la plena eficacia de la Directiva 2000/59/CE. Además, los Estados miembros han desarrollado interpretaciones diferentes de los conceptos esenciales de dicha Directiva, tales como la adecuación de las instalaciones, la notificación previa de desechos, la entrega obligatoria de desechos a instalaciones portuarias receptoras y las exenciones para los buques que operan en tráfico regular. La evaluación REFIT recomendó una mayor armonización de esos conceptos y su plena adaptación al Convenio MARPOL para evitar una carga administrativa innecesaria tanto a los puertos como a sus usuarios.

(13) Con el fin de adaptar la Directiva 2005/35/CE del Parlamento Europeo y del Consejo ([6]) a las disposiciones correspondientes del Convenio MARPOL relativas a las normas sobre descargas, la Comisión debe valorar la conveniencia de revisar dicha Directiva, en particular con miras a ampliar su ámbito de aplicación.

(14) La política marítima de la Unión debe aspirar a un grado elevado de protección del medio ambiente marino habida cuenta de la diversidad de sus zonas marítimas. Debe basarse en el principio de actuación preventiva, en el principio de corrección preferentemente en la fuente misma de los daños causados al medio marino, y en el principio de que quien contamina paga.

(15) La presente Directiva debe desempeñar un papel fundamental en la aplicación de los principios y normas ambientales más importantes en el contexto de los puertos y la gestión de los desechos generados por buques. En particular, las Directivas 2008/56/CE ([7]) y 2008/98/CE ([8]) del Parlamento Europeo y del Consejo son actos pertinentes en este contexto.

(16) La Directiva 2008/98/CE establece los principios esenciales de la gestión de los residuos, incluidos el principio de que «quien contamina paga» y la jerarquía de residuos, que sitúa la reutilización y el reciclado de residuos por delante de otras formas de valorización y eliminación de residuos, y exige el establecimiento de sistemas de recogida separada de residuos. Además, el concepto de responsabilidad ampliada del productor es un principio rector del Derecho de la Unión en materia de residuos, con arreglo al cual los productores son responsables de los efectos medioambientales de sus productos durante todo su ciclo de vida. Esas obligaciones son igualmente aplicables a la gestión de los desechos generados por buques.

([5]) Directiva 2000/60/CE del Parlamento Europeo y del Consejo, de 23 de octubre de 2000, por la que se establece un marco comunitario de actuación en el ámbito de la política de aguas (DO L 327 de 22.12.2000, p. 1).

([6]) Directiva 2005/35/CE del Parlamento Europeo y del Consejo, de 7 de septiembre de 2005, relativa a la contaminación procedente de buques y la introducción de sanciones, incluidas las sanciones penales, para las infracciones de contaminación (DO L 255 de 30.9.2005, p. 11).

([7]) Directiva 2008/56/CE del Parlamento Europeo y del Consejo, de 17 de junio de 2008, por la que se establece un marco de acción comunitaria para la política del medio marino (Directiva marco sobre la estrategia marina) (DO L 164 de 25.6.2008, p. 19).

([8]) Directiva 2008/98/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre los residuos y por la que se derogan determinadas Directivas (DO L 312 de 22.11.2008, p. 3).

(17) La recogida separada de los desechos generados por buques, incluidos los artes de pesca abandonados, es necesaria para asegurar su valorización posterior a fin de poder prepararlos para su reutilización o reciclado en los eslabones siguientes de la cadena de gestión de residuos y para evitar que causen daños a la vida silvestre marina y a los entornos marinos. Los desechos se separan con frecuencia a bordo de los buques de conformidad con las normas internacionales, y el Derecho de la Unión debe garantizar que esos esfuerzos de separación de los desechos a bordo no se dilapiden por falta de medidas para la recogida separada en tierra.

(18) Cada año entra en los mares y océanos de la Unión una importante cantidad de plástico. Aunque, en la mayoría de las zonas marinas, las basuras dispersas en el medio marino tienen su origen en su mayor parte en la actividad terrestre, el sector del transporte marítimo, incluidas la pesca y las actividades de recreo, también contribuye de forma importante con sus descargas de desechos, plásticos y artes de pesca abandonados, que se vierten directamente al mar.

(19) La Directiva 2008/98/CE insta a los Estados miembros a detener los vertidos de basura en el medio marino como contribución al Objetivo de Desarrollo Sostenible de las Naciones Unidas de prevenir y reducir significativamente la contaminación marina de todo tipo.

(20) La Comunicación de la Comisión de 2 de diciembre de 2015 titulada «Cerrar el círculo: un plan de acción de la UE para la economía circular» reconoció el papel específico que debía desempeñar la Directiva 2000/59/CE en este sentido, garantizando la disponibilidad de instalaciones adecuadas para la recepción de desechos y asegurando, al mismo tiempo, un nivel adecuado de incentivos y el control del cumplimiento de la obligación de entregar los desechos a las instalaciones en tierra.

(21) Las instalaciones marinas son una de las fuentes en el mar de vertidos de basuras en el medio marino. Por esta razón, los Estados miembros deben adoptar las medidas que corresponda sobre la entrega de desechos procedentes de aquellas instalaciones marinas que enarbolen su pabellón o que operen en sus aguas, o ambas, y garantizar el cumplimiento de las estrictas normas sobre descargas aplicables a las instalaciones marinas que establece el Convenio MARPOL.

(22) Los desechos, en particular los residuos plásticos, procedentes de los ríos son uno de los principales componentes de la basura dispersa en el medio marino e incluyen las descargas procedentes de los buques de navegación interior. Dichos buques deben estar sujetos a normas estrictas de descarga y entrega. Actualmente, es la comisión fluvial pertinente la que establece esas normas, pero los puertos de navegación interior están cubiertos por el Derecho de la Unión en materia de residuos. A fin de proseguir los esfuerzos de armonización del marco legislativo aplicable a las vías navegables interiores de la Unión, se invita a la Comisión a valorar un régimen de normas de la Unión en materia de descarga y entrega destinado a los buques de navegación interior, que tenga en cuenta el Convenio sobre la recogida, el depósito y la recepción de residuos producidos durante la navegación por el Rin y las vías navegables interiores, de 9 de septiembre de 1996 (CDNI).

(23) Según el Reglamento (CE) n.º 1224/2009 del Consejo ([9]), todos los buques pesqueros de la Unión tienen la obligación de llevar a bordo el equipo para recuperar artes perdidos. En el supuesto de perder artes, el capitán del buque ha de intentar recuperarlos lo antes posible. Si no se pudiera recuperar el arte de pesca, el capitán del buque ha de informar a las autoridades del Estado miembro de su pabellón en un plazo de 24 horas. El Estado miembro del pabellón tiene que comunicarlo entonces a la autoridad competente del Estado miembro ribereño. La información ha de incluir el número de identificación externa y el nombre del buque pesquero, el tipo y la posición del arte de pesca perdido, así como las medidas adoptadas para recuperarlo. Se puede eximir a los buques pesqueros de menos de 12 metros de eslora. En el marco de la propuesta de reglamento del Parlamento Europeo y del Consejo para la modificación del Reglamento (CE) n.º 1224/2009, el buque pesquero debe comunicar la información en un diario electrónico y los Estados miembros deben recoger y registrar la información relativa a los artes perdidos y facilitarla a la Comisión a petición de esta. También podría transmitirse de esta forma la información, recabada y disponible en los recibos de entrega de desechos, sobre los desechos pescados de manera no intencionada, con arreglo a lo dispuesto en la presente Directiva.

(24) El Convenio Internacional para el control y la gestión del agua de lastre y los sedimentos de los buques, que fue adoptado por la OMI el 13 de febrero de 2004 y entró en vigor el 8 de septiembre de 2017, obliga a todos los buques a aplicar procedimientos de gestión del agua de lastre conformes con las normas de la OMI y a los puertos y terminales designados para la limpieza y reparación de tanques de lastre a disponer de instalaciones adecuadas para la recepción de sedimentos.

([9]) Reglamento (CE) n.º 1224/2009 del Consejo, de 20 de noviembre de 2009, por el que se establece un régimen de control de la Unión para garantizar el cumplimiento de las normas de la política pesquera común, se modifican los Reglamentos (CE) n.º 847/96, (CE) n.º 2371/2002, (CE) n.º 811/2004, (CE) n.º 768/2005, (CE) n.º 2115/2005, (CE) n.º 2166/2005, (CE) n.º 388/2006, (CE) n.º 509/2007, (CE) n.º 676/2007, (CE) n.º 1098/2007, (CE) n.º 1300/2008 y (CE) n.º 1342/2008 y se derogan los Reglamentos (CEE) n.º 2847/93, (CE) n.º 1627/94 y (CE) n.º 1966/2006 (DO L 343 de 22.12.2009, p. 1).

(25) Se considera que una instalación portuaria receptora es adecuada si es capaz de satisfacer las necesidades de los buques que utilizan normalmente el puerto, sin causar demoras indebidas, como también se especifica en las Orientaciones refundidas de la OMI y en las Directrices de la OMI para garantizar que las instalaciones y servicios portuarios de recepción de desechos sean adecuados [Resolución MEPC.83(44)]. La adecuación alude tanto a las condiciones operativas de la instalación, habida cuenta de las necesidades de los usuarios, como a la gestión ambiental de las instalaciones en consonancia con el Derecho de la Unión en materia de residuos. En algunos casos podría resultar difícil evaluar si una instalación portuaria receptora situada fuera de la Unión cumple dicha norma.

(26) El Reglamento (CE) n.º 1069/2009 del Parlamento Europeo y del Consejo ([10]) exige la incineración o el enterramiento en un vertedero autorizado de los residuos de cocina internacionales, incluidos los desechos generados por buques en escala en puertos de la Unión que puedan haber estado previamente en contacto con subproductos animales a bordo. Para que este requisito no limite la preparación de la reutilización y el reciclado de los desechos generados por buques, deben hacerse esfuerzos, de conformidad con las Orientaciones refundidas de la OMI, por mejorar la separación de estos, de manera que pueda evitarse la posible contaminación de otros desechos, por ejemplo de los envases de desecho.

(27) Según disponen el Reglamento (CE) n.º 1069/2009, junto con el Reglamento (UE) n.º 142/2011 de la Comisión ([11]), los viajes en el interior de la Unión no se consideran transporte a escala internacional y no es necesario incinerar los residuos de cocina de esos viajes. Ahora bien, dichos viajes dentro de la Unión sí se consideran viajes internacionales en el marco de la legislación marítima internacional [Convenio MARPOL y Convenio Internacional para la Seguridad de la Vida Humana en el Mar (SOLAS)]. A fin de garantizar la coherencia del Derecho de la Unión, a la hora de definir el alcance y el tratamiento de los residuos de cocina internacionales en virtud de la presente Directiva deben seguirse las definiciones del Reglamento (CE) n.º 1069/2009, junto con el Reglamento (UE) n.º 142/2011.

(28) A fin de garantizar la adecuación de las instalaciones portuarias receptoras, resulta esencial desarrollar, ejecutar y reevaluar el plan de recepción y manipulación de desechos basándose en la consulta con todas las partes interesadas. Por razones prácticas y organizativas, es posible que puertos vecinos de una misma región geográfica deseen elaborar un plan conjunto que contemple la disponibilidad de instalaciones portuarias receptoras en cada uno de los puertos comprendidos en el plan, dotado de un marco administrativo común.

(29) En el caso de puertos pequeños no comerciales, como zonas de amarre y puertos deportivos, con poco tráfico —solamente de embarcaciones de recreo—, o que solo se usan durante una parte del año, puede resultar complicado elaborar y supervisar planes de recepción y manipulación de desechos. Los desechos procedentes de estos puertos pequeños suelen quedar a cargo del sistema municipal de gestión de residuos de acuerdo con los principios establecidos en la Directiva 2008/98/CE. Con objeto de no sobrecargar a las autoridades locales y de facilitar la gestión de desechos en estos puertos pequeños, debe ser suficiente que los desechos procedentes de tales puertos se incluyan en el flujo de residuos municipales y se gestionen en consecuencia, que el puerto ponga a disposición de sus usuarios información sobre la recepción de desechos y que los puertos exentos se consignen en un sistema electrónico para permitir un nivel mínimo de control.

(30) Para tratar con eficacia el problema de las basuras dispersas en el medio marino es esencial ofrecer el nivel adecuado de incentivos para la entrega de desechos en las instalaciones portuarias receptoras, en particular de los desechos que figuran en el anexo V del Convenio MARPOL. Esto resulta posible gracias a un sistema de recuperación de los costes que exige la aplicación de una tarifa indirecta. Dicha tarifa indirecta debe abonarse con independencia de si se entregan o no desechos y debe otorgar el derecho de entrega de desechos sin ningún cargo directo adicional. Dada su contribución a la dispersión de basuras en el medio marino, el sector pesquero y el sector recreativo deben quedar obligados al abono de la tarifa indirecta. Sin embargo, en caso de que un buque entregue una cantidad excepcional de los desechos que figuran en el anexo V del Convenio MARPOL, en particular de desechos operacionales, que supere la capacidad máxima específica de almacenamiento indicada en el impreso de notificación previa para la entrega de desechos, debe ser posible cobrar una tarifa directa adicional a fin de lograr que los costes relativos a la recepción de dicha cantidad excepcional de desechos no supongan una carga desproporcionada para el sistema de recuperación de costes de un puerto. Esto mismo puede ocurrir cuando la capacidad específica de almacenamiento declarada resulte excesiva o desproporcionada.

([10]) Reglamento (CE) n.º 1069/2009 del Parlamento Europeo y del Consejo, de 21 de octubre de 2009, por el que se establecen las normas sanitarias aplicables a los subproductos animales y los productos derivados no destinados al consumo humano y por el que se deroga el Reglamento (CE) n.º 1774/2002 (DO L 300 de 14.11.2009, p. 1).

([11]) Reglamento (UE) n.º 142/2011 de la Comisión, de 25 de febrero de 2011, por el que se establecen las disposiciones de aplicación del Reglamento (CE) n.º 1069/2009 del Parlamento Europeo y del Consejo por el que se establecen las normas sanitarias aplicables a los subproductos animales y los productos derivados no destinados al consumo humano, y la Directiva 97/78/CE del Consejo en cuanto a determinadas muestras y unidades exentas de los controles veterinarios en la frontera en virtud de la misma (DO L 54 de 26.2.2011, p. 1).

(31) En algunos Estados miembros se han puesto en marcha programas para proporcionar financiación alternativa de los costes de recogida y gestión de residuos de artes de pesca o desechos pescados de manera no intencionada en tierra, en particular los «programas de pesca de basura». Tales iniciativas deben aplaudirse, y debe alentarse a los Estados miembros a completar los sistemas de recuperación de costes establecidos con arreglo a lo dispuesto en la presente Directiva de manera que los programas de pesca de basura dispersa cubran los costes de la pesca no intencionada de desechos. Estos sistemas de recuperación de los costes, que se basan en la aplicación de una tarifa indirecta del 100 % a los desechos incluidos en el anexo V del Convenio MARPOL, con exclusión de los residuos de carga, no deben por sí mismos desincentivar la participación de las comunidades pesqueras portuarias en los regímenes existentes de entrega de desechos pescados de manera no intencionada.

(32) Las tarifas aplicables a los buques diseñados, equipados o explotados para minimizar los desechos deben reducirse en función de determinados criterios que deben definirse confiriendo a la Comisión competencias de ejecución, en consonancia con las Directrices de la OMI para la implantación del anexo V del Convenio MARPOL y con las normas desarrolladas por la Organización Internacional de Normalización. La reducción y el reciclado eficaz de los desechos se consiguen sobre todo mediante una segregación eficaz de los desechos a bordo con arreglo a dichas directrices y normas.

(33) Debido a su tipo de actividad comercial, que se caracteriza por escalas frecuentes, el transporte marítimo de corta distancia se enfrenta a costes significativos en el marco del régimen vigente por la entrega de desechos en las instalaciones portuarias receptoras, al tener que pagar una tarifa en cada escala. Al mismo tiempo, el tráfico no es lo bastante regular y programado como para acogerse a una exención del pago y de la entrega de desechos por estos motivos. Con el fin de limitar la carga financiera sobre el sector, debe aplicarse una tarifa reducida a los buques en función del tipo de tráfico que practiquen.

(34) Los residuos de carga siguen perteneciendo al propietario de la carga tras la descarga en la terminal y pueden tener un valor económico. Por esa razón, los residuos de carga deben quedar excluidos de los sistemas de recuperación de los costes y de la aplicación de la tarifa indirecta. Los cargos por la entrega de los residuos de carga deben ser abonados por el usuario de la instalación portuaria receptora, tal como especifiquen las disposiciones contractuales entre las partes implicadas u otras disposiciones locales. Los residuos de carga incluyen también los restos de carga líquida oleosa o nociva tras las operaciones de limpieza, a los que se aplican las normas de descarga de los anexos I y II del Convenio MARPOL y que, en determinadas condiciones establecidas en dichos anexos, no necesitan ser entregados en el puerto para evitar costes operativos innecesarios a los buques, así como la congestión de los puertos.

(35) Los Estados miembros deben fomentar la entrega de residuos procedentes del lavado de tanques que contengan sustancias flotantes persistentes de gran viscosidad, posiblemente mediante los incentivos financieros adecuados.

(36) El Reglamento (UE) 2017/352 del Parlamento Europeo y del Consejo ([12]) establece que la disponibilidad de instalaciones portuarias receptoras es un servicio que entra en su ámbito de aplicación. Dicho Reglamento regula la transparencia de las estructuras tarifarias aplicadas para el uso de servicios portuarios, la consulta a los usuarios del puerto y la gestión de los procedimientos de reclamación. La presente Directiva excede del marco establecido por dicho Reglamento por cuanto establece requisitos más detallados sobre el diseño y el funcionamiento de los sistemas de recuperación de los costes aplicables a las instalaciones portuarias receptoras de desechos generados por buques y sobre la transparencia de la estructura de costes.

(37) Además de incentivar la entrega de desechos, es fundamental controlar de manera efectiva la obligación de entrega y hacerlo obedeciendo a un planteamiento basado en los riesgos para el cual debe establecerse un mecanismo de selección de la Unión basado en el riesgo.

(38) Uno de los principales obstáculos al control efectivo del cumplimiento del requisito de entrega obligatoria ha sido la divergencia en la interpretación y aplicación, por parte de los Estados miembros, de la excepción basada en la capacidad de almacenamiento suficiente. Para evitar que su aplicación menoscabe el objetivo primordial de la presente Directiva, debe precisarse la citada excepción, sobre todo en lo que respecta al siguiente puerto de escala, y debe determinarse de manera armonizada la capacidad de almacenamiento suficiente, sobre la base de una metodología y unos criterios comunes. En los casos en que sea difícil determinar si hay disponibles instalaciones portuarias receptoras adecuadas en puertos situados fuera de la Unión, es fundamental que la autoridad competente considere cuidadosamente la aplicación de la excepción.

([12]) Reglamento (UE) 2017/352 del Parlamento Europeo y del Consejo, de 15 de febrero de 2017, por el que se crea un marco para la prestación de servicios portuarios y se adoptan normas comunes sobre la transparencia financiera de los puertos (DO L 57 de 3.3.2017, p. 1).

(39) Ha de lograrse una mayor armonización del régimen de exenciones aplicable a los buques que operan en tráfico regular con escalas frecuentes y regulares; concretamente, deben aclararse los términos empleados y las condiciones que rigen tales exenciones. La evaluación REFIT y la evaluación de impacto han puesto de manifiesto que la falta de armonización en lo relativo a las condiciones y a la aplicación de las exenciones ha generado una carga administrativa innecesaria para los buques y puertos.

(40) El seguimiento y el control del cumplimiento han de facilitarse mediante un sistema basado en la notificación e intercambio de información por vía electrónica. A tal fin, conviene desarrollar el sistema actual de información y seguimiento establecido por la Directiva 2000/59/CE, que debe seguir funcionando sobre la base de los sistemas de datos electrónicos existentes, en particular el sistema de la Unión de intercambio de información marítima (SafeSeaNet) establecido por la Directiva 2002/59/CE del Parlamento Europeo y del Consejo ([13]) y la base de datos de inspecciones establecida por la Directiva 2009/16/CE del Parlamento Europeo y del Consejo ([14]) (Thetis). Dicho sistema debe incorporar también la información sobre las instalaciones portuarias receptoras disponibles en los distintos puertos.

(41) La Directiva 2010/65/UE del Parlamento Europeo y del Consejo ([15]) simplifica y armoniza los procedimientos administrativos aplicados al transporte marítimo mediante la generalización de la transmisión electrónica de datos y la agilización de las formalidades informativas. La Declaración de La Valeta sobre las Prioridades para la política de transporte marítimo de la UE hasta 2020, refrendada por el Consejo en sus Conclusiones de 8 de junio de 2017, invitaba a la Comisión a proponer acciones consecutivas pertinentes para revisar dicha Directiva. La Comisión realizó una consulta pública sobre las formalidades informativas para buques entre el 25 de octubre de 2017 y el 18 de enero de 2018. El 17 de mayo de 2018, la Comisión presentó al Parlamento Europeo y al Consejo una propuesta de reglamento por el que se crea un entorno de ventanilla única marítima europea y se deroga la Directiva 2010/65/UE.

(42) El Convenio MARPOL exige a las Partes Contratantes que mantengan información actualizada sobre sus instalaciones portuarias receptoras y que comuniquen dicha información a la OMI. A tal fin, la OMI ha creado una base de datos de instalaciones portuarias receptoras en el contexto de su sistema mundial integrado de información marítima (GISIS).

(43) En las Orientaciones refundidas de la OMI, esta dispone que se notifiquen las supuestas deficiencias de las instalaciones portuarias receptoras. Con arreglo a ese procedimiento, un buque debe notificar tales deficiencias a la administración del Estado de abanderamiento, que a su vez ha de informar del problema a la OMI y al Estado rector del puerto. El Estado rector del puerto debe estudiar el informe y responder adecuadamente, informando a la OMI y al Estado de abanderamiento que presentó la notificación. Notificar esta información sobre supuestas deficiencias directamente en el sistema de información, seguimiento y control del cumplimiento previsto en la presente Directiva permitiría la transmisión subsiguiente de la información facilitada al GISIS, liberando así a los Estados miembros, ya sean Estados de abanderamiento o rectores de los puertos, de su deber de informar a la OMI.

(44) El subgrupo de instalaciones portuarias receptoras establecido en el marco del Foro Europeo de Navegación Sostenible, que reunió a muy diversos expertos en materia de contaminación por los buques y de gestión de los desechos generados por buques, quedó aplazado en diciembre de 2017 ante el inicio de las negociaciones interinstitucionales. Dado que dicho subgrupo proporcionaba orientaciones y conocimientos valiosos a la Comisión, sería deseable crear un grupo de expertos similar con el mandato de intercambiar experiencias sobre la aplicación de la presente Directiva.

(45) Es importante que todas las sanciones establecidas por los Estados miembros se apliquen correctamente y sean efectivas, proporcionadas y disuasorias.

(46) Unas condiciones laborales adecuadas para el personal que trabaja en las instalaciones portuarias receptoras son de vital importancia para la creación de un sector marítimo seguro, eficiente y socialmente responsable, que sea capaz de atraer a trabajadores cualificados y garantizar una amplia igualdad de condiciones en toda Europa. La formación inicial y periódica del personal es esencial para garantizar la calidad de los servicios y la protección de los trabajadores. Las autoridades portuarias y las autoridades de la instalación portuaria receptora deben velar por que todo el personal reciba la formación necesaria con el fin de adquirir los conocimientos esenciales para su trabajo, prestando una atención particular a los aspectos de salud y seguridad relacionados con la manipulación de materiales peligrosos, y por que los requisitos de formación se actualicen con regularidad para responder a los desafíos de la innovación tecnológica.

([13]) Directiva 2002/59/CE del Parlamento Europeo y del Consejo, de 27 de junio de 2002, relativa al establecimiento de un sistema comunitario de seguimiento y de información sobre el tráfico marítimo y por la que se deroga la Directiva 93/75/CEE del Consejo (DO L 208 de 5.8.2002, p. 10).

([14]) Directiva 2009/16/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre el control de los buques por el Estado rector del puerto (DO L 131 de 28.5.2009, p. 57).

([15]) Directiva 2010/65/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, sobre las formalidades informativas exigibles a los buques a su llegada o salida de los puertos de los Estados miembros y por la que se deroga la Directiva 2002/6/CE (DO L 283 de 29.10.2010, p. 1).

(47) Las competencias conferidas a la Comisión para la ejecución de la Directiva 2000/59/CE deben actualizarse en consonancia con el Tratado de Funcionamiento de la Unión Europea (TFUE).

(48) Deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE, por lo que respecta a la modificación de los anexos de la presente Directiva y las referencias a actos internacionales, en la medida necesaria para adaptarlas de conformidad con el Derecho de la Unión o a fin de tener en cuenta la evolución que se experimente en el plano internacional, en particular en la OMI; a la modificación de los anexos de la presente Directiva cuando sea necesario a fin de mejorar las disposiciones de aplicación y control que establece, en particular en relación con la eficacia de las notificaciones y entregas de desechos, así como la correcta aplicación de las exenciones; también, en circunstancias excepcionales, cuando un análisis adecuado de la Comisión lo justifique adecuadamente y con el fin de evitar una amenaza grave e inevitable al medio ambiente, a la modificación de la presente Directiva en la medida necesaria para eludir tal amenaza, para evitar, en caso necesario, que los cambios en tales actos internacionales se apliquen a los efectos de la presente Directiva. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([16]). En particular, a fin de garantizar una participación equitativa en la elaboración de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(49) A fin de establecer los métodos de cálculo de la capacidad específica de almacenamiento suficiente; desarrollar criterios comunes para reconocer, con objeto de conceder una tarifa por desechos reducida a los buques, que el diseño, equipo y explotación de un buque demuestran que genera cantidades limitadas de desechos y los gestiona de manera sostenible y correcta desde el punto de vista medioambiental; determinar las metodologías para el seguimiento de los datos sobre volúmenes y cantidades de desechos pescados de manera no intencionada, así como el formato para informar; definir los elementos pormenorizados de un mecanismo de selección de la Unión basado en el riesgo, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([17]).

(50) Dado que el objetivo de la presente Directiva, a saber, proteger el medio marino frente a las descargas de desechos en el mar, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a la dimensión de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dicho objetivo.

(51) En lo que respecta a los puertos, la Unión se caracteriza por las disparidades regionales, tal como ha corroborado la evaluación de impacto territorial llevada a cabo por la Comisión. Los puertos presentan diferencias en cuanto a situación geográfica, tamaño, estructura administrativa y propiedad, y se caracterizan en función del tipo de buques que recalan normalmente en ellos. Además, los sistemas de gestión de desechos reflejan las diferencias en el plano municipal y en lo relativo a las infraestructuras de gestión posterior de los desechos.

(52) El artículo 349 del TFUE exige que se tengan en cuenta las características especiales de las regiones ultraperiféricas de la Unión, a saber, Guadalupe, la Guayana Francesa, Martinica, la Reunión, San Bartolomé, San Martín, las Azores, Madeira y las islas Canarias. Para garantizar la adecuación y disponibilidad de las instalaciones portuarias receptoras, puede ser adecuado que los Estados miembros pongan a disposición de los operadores de las instalaciones portuarias receptoras o de las autoridades portuarias en esas regiones de la Unión una ayuda regional de funcionamiento, a fin de hacer frente a los efectos de las desventajas permanentes a que se refiere dicho artículo. La ayuda regional de funcionamiento que facilitan los Estados miembros en este contexto está exenta de la obligación de notificación establecida en el artículo 108, apartado 3, del TFUE si, en el momento de la concesión, cumple las condiciones establecidas en el Reglamento (UE) n.º 651/2014 de la Comisión ([18]) por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado, adoptado de conformidad con el Reglamento (CE) n.º 994/98 del Consejo ([19]).

(53) Por consiguiente, debe derogarse la Directiva 2000/59/CE.

([16]) DO L 123 de 12.5.2016, p. 1.

([17]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

([18]) Reglamento (UE) n.º 651/2014 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado (DO L 187 de 26.6.2014, p. 1).

([19]) Reglamento (CE) n.º 994/98 del Consejo de 7 de mayo de 1998 sobre la aplicación de los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea a determinadas categorías de ayudas estatales horizontales (DO L 142 de 14.5.1998, p. 1).

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Sección 1

Disposiciones generales

Artículo 1

Objeto

La presente Directiva tiene por objeto proteger el medio marino de las repercusiones negativas de las descargas de desechos por los buques que utilizan los puertos situados en la Unión, al tiempo que se garantiza el buen funcionamiento del tráfico marítimo, mejorando la disponibilidad y la utilización de instalaciones portuarias receptoras adecuadas y la entrega de desechos a dichas instalaciones.

Artículo 2

Definiciones

A los efectos de la presente Directiva, se entenderá por:

1) «buque»: todo tipo de nave de navegación marítima que opere en el medio marino, incluidos los buques de pesca, las embarcaciones de recreo, los aliscafos, aerodeslizadores, sumergibles y artefactos flotantes;

2) «Convenio MARPOL»: el Convenio internacional para prevenir la contaminación ocasionada por los buques, en su versión vigente;

3) «desechos generados por buques»: todos los desechos, incluidos los residuos de carga, que se generen durante el servicio de un buque o durante operaciones de carga, descarga y limpieza y que entran en el ámbito de aplicación de los anexos I, II, IV, V y VI del Convenio MARPOL, así como los desechos pescados de manera no intencionada;

4) «desechos pescados de manera no intencionada»: los desechos recogidos en las redes durante operaciones de pesca;

5) «residuos de carga»: los restos de cualquier material de carga embarcado que queden en la cubierta, en las bodegas o en los tanques tras las operaciones de carga y descarga, incluidos el exceso o el derramamiento en la carga y descarga, ya sea en estado seco o húmedo o arrastrados en el agua de lavado, excluido el polvo de la carga que quede en la cubierta tras el barrido o el polvo depositado en las superficies exteriores del buque;

6) «instalación portuaria receptora»: toda instalación fija, flotante o móvil capaz de prestar el servicio de recepción de desechos generados por buques;

7) «buque de pesca»: todo buque equipado o utilizado a efectos comerciales para la captura de peces u otros recursos vivos del mar;

8) «embarcación de recreo»: todo tipo de embarcación con una eslora de 2,5 metros o superior, con independencia de su medio de propulsión, destinada a fines deportivos o recreativos y que no realiza actividades comerciales;

9) «puerto»: un lugar o una zona geográfica que presente obras de mejora y dotado de equipo diseñado principalmente para permitir la recepción de buques, incluido el fondeadero dentro de la jurisdicción del puerto;

10) «capacidad de almacenamiento suficiente»: la capacidad suficiente para almacenar desechos a bordo desde el momento de salir del puerto hasta el siguiente puerto de escala, incluidos los desechos que probablemente vayan a generarse durante el viaje;

11) «tráfico regular»: el tráfico basado en una lista publicada o programada de horas de salida y de llegada entre puertos determinados o las travesías recurrentes que constituyan un programa horario reconocido;

12) «escalas regulares»: los trayectos repetidos del mismo buque que formen un patrón constante entre puertos determinados o una serie de viajes con salida y destino en el mismo puerto sin escalas intermedias;

13) «escalas frecuentes»: las escalas de un buque en el mismo puerto al menos una vez por quincena;

14) «GISIS»: el sistema mundial integrado de información marítima establecido por la OMI;

15) «tratamiento»: las operaciones de valorización o eliminación, incluida la preparación anterior a la valorización o eliminación;

16) «tarifa indirecta»: una tarifa abonada por la prestación de servicios por parte de las instalaciones portuarias receptoras, independientemente de la entrega efectiva de desechos generados por buques.

Los «desechos generados por buques» mencionados en el punto 3 se considerarán residuos en la acepción del artículo 3, punto 1, de la Directiva 2008/98/CE.

Artículo 3

Ámbito de aplicación

1. La presente Directiva se aplicará a:

a) todo buque, con independencia del pabellón que enarbole, que haga escala u opere en un puerto de un Estado miembro, excepto los buques que participen en servicios portuarios en el sentido del artículo 1, apartado 2, del Reglamento (UE) 2017/352, y excepto los buques de guerra, unidades navales auxiliares u otros buques que, siendo propiedad de un Estado o estando a su servicio, solo presten por el momento servicios públicos de carácter no comercial;

b) todos los puertos de los Estados miembros en los que normalmente hagan escala los buques incluidos en el ámbito de aplicación de la letra a).

A efectos de la presente Directiva y para evitar demoras indebidas a los buques, los Estados miembros podrán decidir excluir los fondeaderos de sus puertos a efectos de la aplicación de los artículos 6, 7 y 8.

2. Los Estados miembros adoptarán medidas para garantizar que, en la medida de lo razonablemente posible, los buques excluidos del ámbito de aplicación de la presente Directiva descarguen sus desechos de manera compatible con la presente Directiva.

3. Los Estados miembros que carezcan de puertos o de buques que enarbolen su pabellón y que se incluyan en el ámbito de aplicación de la presente Directiva podrán quedar exentos de las disposiciones de esta última, a excepción de la obligación establecida en el párrafo tercero del presente apartado.

Los Estados miembros que carezcan de puertos que se incluyan en el ámbito de aplicación de la presente Directiva podrán quedar exentos de aquellas disposiciones de esta que se refieran exclusivamente a los puertos.

Aquellos Estados miembros que deseen acogerse a las exenciones establecidas en el presente apartado comunicarán a la Comisión a más tardar el 28 de junio de 2021 si se cumplen las condiciones aplicables y, a continuación, informarán a la Comisión anualmente de cualquier cambio posterior. Hasta que dichos Estados miembros no hayan transpuesto y aplicado la presente Directiva, no podrán tener puertos que se incluyan en el ámbito de aplicación de la presente Directiva ni podrán permitir que enarbolen su pabellón aquellos buques, o embarcaciones, que se incluyan en el ámbito de aplicación de la presente Directiva.

Sección 2

Disponibilidad de instalaciones portuarias receptoras adecuadas

Artículo 4

Instalaciones portuarias receptoras

1. Los Estados miembros garantizarán que se disponga de instalaciones portuarias receptoras adecuadas que satisfagan las necesidades de los buques que utilicen normalmente el puerto y no causen demoras innecesarias a los buques.

2. Los Estados miembros garantizarán que:

a) las instalaciones portuarias receptoras tengan capacidad para recibir los tipos y cantidades de desechos generados por los buques que utilicen normalmente ese puerto, tomando en consideración:

   i) las necesidades operativas de los usuarios del puerto,

   ii) el tamaño y la situación geográfica del puerto,

   iii) el tipo de buques que hagan escala en el puerto, y

   iv) las exenciones previstas en el artículo 9;

b) los trámites y las disposiciones prácticas para la utilización de las instalaciones portuarias receptoras sean sencillos y rápidos para evitar demoras innecesarias a los buques;

c) las tarifas aplicadas a las entregas no desincentiven la utilización de las instalaciones portuarias receptoras por parte de los buques; y

d) las instalaciones portuarias receptoras hagan posible la gestión de los desechos generados por buques de forma respetuosa con el medio ambiente de conformidad con la Directiva 2008/98/CE y otras normas de la Unión y nacionales aplicables en materia de residuos.

A los efectos de la letra d) del párrafo primero, los Estados miembros garantizarán la recogida separada de los desechos generados por buques en los puertos para facilitar su reutilización y reciclado, tal como exija el Derecho de la Unión en materia de residuos, en particular la Directiva 2006/66/CE del Parlamento Europeo y del Consejo ([20]), la Directiva 2008/98/CE y la Directiva 2012/19/UE del Parlamento Europeo y del Consejo ([21]). A fin de facilitar este proceso, las instalaciones portuarias receptoras podrán recoger las fracciones de desechos por separado de conformidad con las categorías de desechos definidas en el Convenio MARPOL, teniendo en cuenta las directrices de este.

La letra d) del párrafo primero se aplicará sin perjuicio de los requisitos más estrictos establecidos en el Reglamento (CE) n.º 1069/2009 en lo que respecta a la gestión de los residuos de cocina procedentes del transporte internacional.

3. Los Estados miembros, en su calidad de Estados de abanderamiento, utilizarán los formularios y procedimientos de la OMI para notificar a esta y a las autoridades del Estado rector del puerto las supuestas deficiencias de las instalaciones portuarias receptoras.

Los Estados miembros, en su calidad de Estados rectores de los puertos, investigarán todos los casos de supuestas deficiencias comunicados y utilizarán los formularios y procedimientos de la OMI para notificar los resultados de la investigación a la OMI y al Estado de abanderamiento que informó.

4. Las autoridades portuarias correspondientes, o en su defecto las autoridades pertinentes, garantizarán que las operaciones de entrega o recepción de desechos se realicen con las suficientes medidas de seguridad para evitar riesgos tanto personales como medioambientales en los puertos incluidos en el ámbito de aplicación de la presente Directiva.

5. Los Estados miembros garantizarán que toda parte dedicada a la entrega o recepción de desechos generados por buques pueda exigir una indemnización por los daños causados por una demora innecesaria.

([20]) Directiva 2006/66/CE del Parlamento Europeo y del Consejo, de 6 de septiembre de 2006, relativa a las pilas y acumuladores y a los residuos de pilas y acumuladores y por la que se deroga la Directiva 91/157/CEE (DO L 266 de 26.9.2006, p. 1).

([21]) Directiva 2012/19/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, sobre residuos de aparatos eléctricos y electrónicos (RAEE) (DO L 197 de 24.7.2012, p. 38).

Artículo 5

Planes de recepción y manipulación de desechos

1. Los Estados miembros garantizarán que se elabore y aplique en cada puerto un plan de recepción y manipulación de desechos adecuado al término de consultas con las partes interesadas, entre las cuales han de contarse, en particular, los usuarios del puerto o sus representantes, y, cuando proceda, las autoridades locales competentes, los operadores de las instalaciones portuarias receptoras, las organizaciones que apliquen las obligaciones en materia de responsabilidad ampliada del productor y los representantes de la sociedad civil. Esas consultas se celebrarán tanto durante la elaboración inicial del plan de recepción y manipulación de desechos como tras su adopción, en particular, cuando se hayan introducido cambios significativos, por lo que respecta a los requisitos de los artículos 4, 6 y 7.

En el anexo 1 se pormenorizan los requisitos para la elaboración de los planes de recepción y manipulación de desechos.

2. Los Estados miembros garantizarán que se comunique con claridad a los operadores de los buques, se ponga a disposición del público y sea fácilmente accesible, en una lengua oficial del Estado miembro en el que esté situado el puerto y, cuando proceda, en una lengua que se utilice internacionalmente, la información siguiente, relativa a la disponibilidad de instalaciones portuarias receptoras adecuadas en sus puertos y a la estructura de los costes, que figura en los planes de recepción y manipulación de desechos:

a) situación de las instalaciones portuarias receptoras correspondientes a cada muelle, y, cuando proceda, el horario de apertura;

b) lista de los desechos generados por buques, gestionados normalmente por el puerto;

c) lista de los puntos de contacto, los operadores de las instalaciones portuarias receptoras y los servicios ofrecidos;

d) descripción de los procedimientos de entrega de desechos;

e) descripción de los sistemas de recuperación de los costes, incluyendo los regímenes y financiación para la gestión de desechos mencionados en el anexo 4, cuando proceda.

La información a que se refiere el párrafo primero del presente apartado se facilitará también por vía electrónica y se mantendrá actualizada en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13.

3. Cuando así lo aconsejen razones de eficiencia, dos o más puertos vecinos de la misma región geográfica podrán elaborar conjuntamente los planes de recepción y manipulación de desechos, con la adecuada participación de cada puerto, siempre que se especifique la necesidad y disponibilidad de instalaciones portuarias receptoras para cada uno de los puertos.

4. Los Estados miembros evaluarán y aprobarán el plan de recepción y manipulación de desechos y se asegurarán de que se realiza un nuevo proceso de aprobación al menos cada cinco años tras su aprobación inicial o última aprobación, y cada vez que se introduzcan cambios significativos en el funcionamiento del puerto. Esos cambios podrán incluir cambios estructurales en el tráfico del puerto, desarrollo de nuevas infraestructuras, modificaciones en la demanda y oferta de instalaciones portuarias receptoras y nuevas técnicas de tratamiento a bordo.

Los Estados miembros supervisarán la aplicación del plan de recepción y manipulación de desechos por parte del puerto. Si en los cinco años a que se refiere el párrafo primero no se produce ningún cambio significativo, el nuevo proceso de aprobación podrá consistir en la validación de los planes existentes.

5. Los puertos pequeños no comerciales caracterizados por un tráfico raro o escaso constituido por embarcaciones de recreo solo podrán quedar exentos de los apartados 1 a 4, si sus instalaciones portuarias receptoras están integradas en el sistema de gestión de desechos gestionado por el municipio correspondiente o por cuenta de este y si los Estados miembros en los que estén situados esos puertos garantizan que la información sobre el sistema de gestión de desechos se pone a la disposición de los usuarios de dichos puertos.

Los Estados miembros en los que estén situados esos puertos notificarán el nombre y la ubicación de dichos puertos por vía electrónica en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13.

Sección 3

Entrega de desechos generados por buques

Artículo 6

Notificación previa de desechos

1. El operador, agente o capitán de un buque incluido en el ámbito de aplicación de la Directiva 2002/59/CE que se dirija a un puerto de la Unión cumplimentará con veracidad y exactitud el formulario establecido en el anexo 2 de la presente Directiva («notificación previa de desechos») y notificará toda la información contenida en dicho formulario a la autoridad u organismo designado a tal fin por el Estado miembro en cuyo territorio esté situado el puerto:

a) como mínimo veinticuatro horas antes de llegar, si se conoce el puerto de escala;

b) en cuanto se conozca el puerto de escala, si se dispone de esa información menos de veinticuatro horas antes de la llegada; o

c) a más tardar en el momento de salir del puerto anterior, si la duración del viaje es inferior a veinticuatro horas.

2. La información de la notificación previa de desechos se comunicará por vía electrónica en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13 de la presente Directiva, de conformidad con las Directivas 2002/59/CE y 2010/65/UE.

3. La información de la notificación previa de desechos estará disponible a bordo, preferiblemente en formato electrónico, al menos hasta el siguiente puerto de escala y se pondrá a disposición de las autoridades competentes de los Estados miembros que la soliciten.

4. Los Estados miembros garantizarán que la información notificada con arreglo al presente artículo se examine y se comparta sin demora con las autoridades competentes en materia de control del cumplimiento.

Artículo 7

Entrega de desechos generados por buques

1. El capitán de todo buque que haga escala en un puerto de la Unión entregará a una instalación portuaria receptora, antes de abandonar el puerto, todos los desechos que lleve a bordo de conformidad con las normas pertinentes en materia de descargas establecidas en el Convenio MARPOL.

2. Tras la entrega, el operador de la instalación portuaria receptora o la autoridad del puerto en el que se proceda a la entrega cumplimentará con veracidad y exactitud el formulario establecido en el anexo 3 («recibo de entrega de desechos») y expedirá y entregará, sin demora innecesaria, el recibo de entrega de desechos al capitán del buque.

El requisito establecido en el párrafo primero no se aplicará en los puertos pequeños con instalaciones sin dotación de personal ni en los que se sitúen en lugares remotos, siempre y cuando el Estado miembro en el que estén situados dichos puertos haya notificado el nombre y la ubicación de dichos puertos por vía electrónica en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13.

3. El operador, agente o capitán de un buque incluido en el ámbito de aplicación de la Directiva 2002/59/CE comunicará por vía electrónica, antes de salir del puerto o en cuanto haya recibido el recibo de entrega de desechos, la información contenida en este en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13 de la presente Directiva, de conformidad con las Directivas 2002/59/CE y 2010/65/UE.

La información del recibo de entrega de desechos estará disponible a bordo durante al menos dos años, en su caso, junto con el correspondiente Libro de registro de hidrocarburos, Libro de registro de carga y Libro de registro de basuras o con el plan de gestión de basuras, y se facilitará a petición de las autoridades de los Estados miembros.

4. Sin perjuicio de lo dispuesto en el apartado 1, todo buque podrá dirigirse hacia el siguiente puerto de escala sin entregar los desechos si:

a) de la información facilitada de conformidad con los anexos 2 y 3 se deduce que existe una capacidad específica de almacenamiento suficiente para todos los desechos que se hayan acumulado y que vayan a acumularse durante el viaje previsto del buque hasta el siguiente puerto de escala;

b) de la información disponible a bordo de los buques excluidos del ámbito de aplicación de la Directiva 2002/59/CE se deduce que existe una capacidad específica de almacenamiento suficiente para todos los desechos que se hayan acumulado y que vayan a acumularse durante el viaje previsto del buque hasta el siguiente puerto de escala; o

c) el buque se limita a hacer escala en fondeadero durante menos de veinticuatro horas o en condiciones meteorológicas adversas, a menos que dicha zona haya quedado excluida de conformidad con el artículo 3, apartado 1, párrafo segundo.

Con objeto de garantizar condiciones uniformes de ejecución de la excepción a que se refiere el párrafo primero, letras a) y b), la Comisión adoptará actos de ejecución para determinar los métodos que deban emplearse para el cálculo de la capacidad específica de almacenamiento suficiente. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 20, apartado 2.

5. El Estado miembro exigirá al buque la entrega de todos sus desechos antes de salir del puerto si:

a) no se puede determinar, según la información disponible, incluida la información disponible por vía electrónica en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13 o en el GISIS, que el siguiente puerto de escala dispone de instalaciones portuarias receptoras adecuadas, o

b) se desconoce el siguiente puerto de escala.

6. El apartado 4 se aplicará sin perjuicio de disposiciones más rigurosas para los buques adoptadas de conformidad con el Derecho internacional.

Artículo 8

Sistemas de recuperación de costes

1. Los Estados miembros garantizarán que los costes de gestión de las instalaciones portuarias receptoras relativos a la entrega y el tratamiento de desechos generados por buques, distintos de los residuos de carga, se sufraguen mediante el cobro de una tarifa a los buques. Esos costes incluirán los elementos enumerados en el anexo 4.

2. Los sistemas de recuperación de los costes no deberán constituir un incentivo para que los buques viertan sus desechos en el mar. A tal fin, los Estados miembros aplicarán en el diseño y funcionamiento de los sistemas de recuperación de los costes los principios que figuran a continuación:

a) los buques abonarán una tarifa indirecta, con independencia de si se entregan o no desechos a una instalación portuaria receptora;

b) la tarifa indirecta cubrirá:

   i) los costes administrativos indirectos,

   ii) una proporción significativa de los costes operativos directos indicados en el anexo 4 que representará al menos el 30 % del total de los costes directos de la entrega efectiva de desechos del año anterior, con la posibilidad de tener en cuenta también los costes relativos al volumen de tráfico previsto para el año siguiente;

c) con el fin de ofrecer un incentivo máximo a la entrega de los desechos del anexo V del Convenio MARPOL distintos de los residuos de carga, no se cobrará ninguna tarifa directa sobre dichos desechos, a fin de garantizar un derecho de entrega sin ningún coste adicional basado en el volumen de desechos entregados, excepto cuando dicho volumen supere la capacidad máxima específica de almacenamiento indicada en el formulario establecido en el anexo 2 de la presente Directiva; este régimen cubrirá los desechos pescados de manera no intencionada, en particular en lo relativo al derecho de entrega;

d) para evitar que los costes de recogida y tratamiento de los desechos pescados de manera no intencionada corran exclusivamente a cargo de los usuarios de los puertos, los Estados miembros cubrirán, cuando proceda, dichos costes a partir de los ingresos generados por sistemas de financiación alternativos, entre ellos, por los regímenes de gestión de desechos y por la financiación disponible de la Unión, nacional o regional;

e) con objeto de fomentar la entrega de residuos procedentes del lavado de tanques que contengan sustancias flotantes persistentes de gran viscosidad, los Estados miembros podrán proporcionar los incentivos financieros adecuados para su entrega;

f) la tarifa indirecta no incluirá los desechos de los sistemas de limpieza de los gases de escape, cuyos costes se cubrirán en función de los tipos y cantidades de desechos entregados.

3. En su caso, la parte de los costes no cubierta por la tarifa indirecta se cubrirá en función de los tipos y cantidades de desechos entregados realmente por el buque.

4. Las tarifas podrán diferenciarse en función de los siguientes elementos:

a) la categoría, el tipo y el tamaño del buque;

b) la prestación de servicios a buques fuera de los horarios normales de funcionamiento del puerto; o

c) la naturaleza peligrosa de los desechos.

5. Las tarifas se reducirán en función de los siguientes elementos:

a) el tipo de actividad comercial que realice el buque, en particular cuando se trate de transporte marítimo comercial de corta distancia;

b) el diseño, el equipo y la explotación del buque demuestren que el buque genera cantidades limitadas de desechos y gestiona sus desechos de manera sostenible y respetuosa del medio ambiente.

A más tardar el 28 de junio de 2020, la Comisión adoptará actos de ejecución para desarrollar los criterios para determinar si un buque reúne los requisitos enunciados en la letra b) del párrafo primero respecto de la gestión de los desechos a bordo del buque. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 20, apartado 2.

6. Para garantizar que las tarifas sean equitativas, transparentes, fáciles de identificar y no discriminatorias, y reflejen los costes de las instalaciones y los servicios que se ofrecen y, en su caso, se utilizan, los importes de las tarifas y las bases de cálculo correspondientes se pondrán a disposición de los usuarios del puerto en los planes de recepción y manipulación de desechos en una lengua oficial del Estado miembro en el que esté situado el puerto y, cuando proceda, en una lengua que se utilice internacionalmente.

7. Los Estados miembros garantizarán que se recojan los datos de seguimiento sobre el volumen y la cantidad de desechos pescados de manera no intencionada y transmitirán dichos datos de seguimiento a la Comisión. La Comisión publicará, sobre la base de dichos datos de seguimiento, un informe a más tardar el 31 de diciembre de 2022 y posteriormente cada dos años.

La Comisión adoptará actos de ejecución para determinar la metodología aplicable a los datos de seguimiento y el formato de su comunicación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 20, apartado 2.

Artículo 9

Exenciones

1. Los Estados miembros podrán eximir a todo buque que haga escala en sus puertos de las obligaciones establecidas en el artículo 6, el artículo 7, apartado 1, y el artículo 8 (en lo sucesivo, «exención»), cuando se disponga de pruebas suficientes de que se cumplen los requisitos siguientes:

a) el buque opera en tráfico regular con escalas frecuentes y regulares;

b) existe un acuerdo que asegura la entrega de los desechos y el pago de las tarifas en uno de los puertos situados en su ruta, acuerdo que:

   i) está acreditado por un contrato firmado con un puerto o un contratista de desechos y por recibos de entrega de desechos,

   ii) ha sido comunicado a todos los puertos situados en la ruta del buque, y

   iii) ha sido aceptado por el puerto donde se realiza la entrega y el pago, que puede ser un puerto de la Unión u otro puerto en el que se dispone de instalaciones adecuadas, según se ha determinado sobre la base de la información transmitida por vía electrónica en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13 y al GISIS;

c) la exención no tiene repercusiones negativas en la seguridad marítima, la salud, las condiciones de vida o de trabajo a bordo o el medio marino.

2. Si se concede la exención, el Estado miembro en el que esté situado el puerto expedirá un certificado de exención, basado en el modelo que figura en el anexo 5, que confirme que el buque reúne las condiciones y los requisitos necesarios para la aplicación de la exención y que indique la duración de esta.

3. Los Estados miembros comunicarán por vía electrónica la información contenida en el certificado de exención en la parte del sistema de información, seguimiento y control del cumplimiento a que se refiere el artículo 13.

4. Los Estados miembros garantizarán la eficacia de la supervisión y el control del cumplimiento de los acuerdos de entrega y pago vigentes para los buques exentos que visiten sus puertos.

5. No obstante la exención concedida, un buque no podrá dirigirse hacia el siguiente puerto de escala si la capacidad específica de almacenamiento es insuficiente para todos los desechos que se hayan acumulado y que vayan a acumularse durante el viaje previsto del buque hasta el siguiente puerto de escala.

Sección 4

Control del cumplimiento

Artículo 10

Inspecciones

Los Estados miembros garantizarán que todo buque pueda ser sometido a inspecciones, que podrán ser aleatorias, para comprobar que cumple la presente Directiva.

Artículo 11

Compromisos de inspección

1. Los Estados miembros procederán a inspecciones de los buques que hacen escala en sus puertos en una proporción mínima del 15 % del número total de unidades de buques que hagan escala anualmente en sus puertos.

El número total de unidades de buques que hacen escala en un Estado miembro será el resultado del cálculo del número medio de unidades de buques que lo hayan hecho durante los tres años anteriores, según lo registrado en la parte del sistema de información, seguimiento y control del cumplimiento a que hace referencia el artículo 13.

2. Los Estados miembros cumplirán el apartado 1 del presente artículo seleccionando buques con arreglo a un mecanismo de selección de la Unión basado en el riesgo.

Con objeto de garantizar la armonización de las inspecciones y facilitar condiciones uniformes de selección de los buques para su inspección, la Comisión adoptará actos de ejecución para determinar los elementos pormenorizados de un mecanismo de selección de la Unión basado en el riesgo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 20, apartado 2.

3. Los Estados miembros establecerán procedimientos para la realización de inspecciones a los buques excluidos del ámbito de aplicación de la Directiva 2002/59/CE a fin de garantizar, en la medida de lo posible, el cumplimiento de la presente Directiva.

A la hora de establecer dichos procedimientos, los Estados miembros podrán tener en cuenta el mecanismo de selección de la Unión basado en el riesgo, al que se refiere el apartado 2.

4. Si la autoridad competente del Estado miembro no queda satisfecha de los resultados de la inspección, se asegurará, sin perjuicio de la aplicación de las sanciones mencionadas en el artículo 16, de que el buque no salga de puerto hasta que haya entregado sus desechos a una instalación portuaria receptora conforme a lo dispuesto en el artículo 7.

Artículo 12

Sistema de información, seguimiento y control del cumplimiento

La aplicación y el control del cumplimiento de la presente Directiva se facilitarán mediante la comunicación y el intercambio de información por vía electrónica entre los Estados miembros de conformidad con los artículos 13 y 14.

Artículo 13

Comunicación e intercambio de información

1. La comunicación y el intercambio de información se basarán en el sistema de la Unión de intercambio de información marítima (SafeSeaNet) a que se refieren el artículo 22 *bis*, apartado 3, y el anexo III de la Directiva 2002/59/CE.

2. Los Estados miembros garantizarán que se comunique por vía electrónica y en un plazo razonable, de conformidad con la Directiva 2010/65/UE, la información siguiente:

a) la información relativa a la hora de llegada real y la hora de salida real de todo buque comprendido en el ámbito de aplicación de la Directiva 2002/59/CE que haga escala en un puerto de la Unión, junto con un identificador de dicho puerto;

b) la información contenida en la notificación previa de desechos, según figura en el anexo 2;

c) la información contenida en el recibo de entrega de desechos, según figura en el anexo 3;

d) la información contenida en el certificado de exención, según figura en el anexo 5.

3. Los Estados miembros garantizarán que la información enumerada en el artículo 5, apartado 2, esté disponible por vía electrónica en el sistema SafeSeaNet.

Artículo 14

Registro de inspecciones

1. La Comisión elaborará, mantendrá y actualizará una base de datos de inspecciones a la que todos los Estados miembros estarán conectados y que contendrá toda la información necesaria para la aplicación del sistema de inspección previsto en la presente Directiva (en lo sucesivo, «base de datos de inspecciones»). La base de datos de inspecciones se ajustará a la base de datos de inspecciones a que se refiere el artículo 24 de la Directiva 2009/16/CE y tendrá funciones similares a las de dicha base de datos.

2. Los Estados miembros se asegurarán de que la información relativa a las inspecciones en el marco de la presente Directiva, incluida la información sobre los casos de incumplimiento y sobre las órdenes de prohibición de salida emitidas, se transfiera sin demora a la base de datos de inspecciones tan pronto como:

a) se haya completado el informe de inspección,

b) se haya levantado la orden de prohibición de salida, o

c) se haya concedido una exención.

3. La Comisión garantizará que la base de datos de inspecciones permita recuperar todos los datos pertinentes comunicados por los Estados miembros a efectos de la supervisión de la aplicación de la presente Directiva.

La Comisión garantizará que la base de datos de inspecciones facilite información para el mecanismo de selección de la Unión basado en el riesgo a que se refiere el artículo 11, apartado 2.

La Comisión revisará periódicamente la base de datos de inspecciones para hacer un seguimiento de la aplicación de la presente Directiva y llamará la atención sobre cualquier posible duda por lo que respecta a su aplicación integral con el fin de fomentar la adopción de medidas correctoras.

4. Los Estados miembros tendrán acceso en todo momento a la información registrada en la base de datos de inspecciones.

Artículo 15

Formación del personal

Las autoridades portuarias y las autoridades de las instalaciones portuarias receptoras garantizarán que todo el personal reciba la formación necesaria al objeto de adquirir los conocimientos esenciales para su trabajo en lo que respecta a manejar desechos, prestando una atención particular a los aspectos de salud y seguridad relacionados con la manipulación de materiales peligrosos, y por que los requisitos de formación se actualicen periódicamente para responder a los desafíos de la innovación tecnológica.

Artículo 16

Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables a cualquier infracción de las disposiciones nacionales adoptadas al amparo de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su ejecución. Tales sanciones serán efectivas, proporcionadas y disuasorias.

Sección 5

Disposiciones finales

Artículo 17

Intercambio de experiencias

La Comisión velará por que se organicen entre las autoridades nacionales de los Estados miembros y los expertos, incluidos los del sector privado, la sociedad civil y los sindicatos, intercambios sobre su experiencia en la aplicación de la presente Directiva en los puertos de la Unión.

Artículo 18

Procedimiento de modificación

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 19 con el fin de modificar los anexos de la presente Directiva y las referencias a actos de la OMI en la presente Directiva, en la medida de lo necesario para adaptarlos al Derecho de la Unión o para tomar en consideración la evolución internacional, en particular en el plano de la OMI.

2. La Comisión también estará facultada para adoptar actos delegados con arreglo al artículo 19 con el fin de modificar los anexos cuando resulte necesario a efectos de mejorar las modalidades de aplicación y supervisión establecidas en la presente Directiva, y en particular las previstas en sus artículos 6, 7 y 9, con objeto de asegurar la notificación y entrega efectivas de desechos y la correcta aplicación de las exenciones.

3. En circunstancias excepcionales, cuando esté debidamente justificado por un análisis adecuado realizado por la Comisión y con el fin de evitar una amenaza grave e inaceptable para el medio marino, la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 19 a fin de modificar la presente Directiva en la medida de lo necesario para evitar tal amenaza, con el fin de no aplicar, a los efectos de la presente Directiva, alguna enmienda del Convenio MARPOL.

4. Los actos delegados mencionados en el presente artículo se adoptarán al menos tres meses antes de que expire el plazo establecido internacionalmente para la aceptación tácita de la enmienda al Convenio MARPOL o de la fecha prevista para su entrada en vigor.

En el período previo a la entrada en vigor de dichos actos delegados, los Estados miembros se abstendrán de toda iniciativa tendente a integrar en el Derecho nacional o aplicar la enmienda al acto internacional de que se trate.

Artículo 19

Ejercicio de la delegación

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

2. Los poderes para adoptar actos delegados mencionados en el artículo 18, apartados 1, 2 y 3, se otorgan a la Comisión por un período de cinco años a partir del 27 de junio de 2019. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 18, apartados 1, 2 y 3, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

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

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

6. Los actos delegados adoptados en virtud del artículo 18, apartados 1, 2 y 3, entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 20

Procedimiento de comité

1. La Comisión estará asistida por el Comité de seguridad marítima y prevención de la contaminación por los buques (COSS) establecido en virtud del Reglamento (CE) n.º 2099/2002 del Parlamento Europeo y del Consejo ([22]). Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 21

Modificación de la Directiva 2010/65/UE

En la sección A del anexo de la Directiva 2010/65/UE, el punto 4 se sustituye por el texto siguiente:

«4. Notificación de desechos generados por buques, incluidos otros residuos

Artículos 6, 7 y 9 de la Directiva (UE) 2019/883 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativa a las instalaciones portuarias receptoras a efectos de la entrega de desechos generados por buques, por la que se modifica la Directiva 2010/65/UE y se deroga la Directiva 2000/59/CE (DO L 151 de 7.6.2019, p. 116).».

Artículo 22

Derogación

Queda derogada la Directiva 2000/59/CE.

Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva.

Artículo 23

Revisión

1. La Comisión evaluará la presente Directiva y transmitirá los resultados de la evaluación al Parlamento Europeo y al Consejo a más tardar el 28 de junio de 2026. La evaluación incluirá también un informe en el que se detallarán las mejores prácticas en materia de prevención y gestión de desechos a bordo de buques.

2. En el contexto del Reglamento (UE) 2016/1625 del Parlamento Europeo y del Consejo ([23]), cuando haya que llevar a cabo la próxima revisión del mandato de la Agencia Europea de Seguridad Marítima (AESM), la Comisión evaluará asimismo si deben atribuirse nuevas competencias a la AESM para el control del cumplimiento de la presente Directiva.

([22]) Reglamento (CE) n.º 2099/2002 del Parlamento Europeo y del Consejo, de 5 de noviembre de 2002, por el que se crea el Comité de seguridad marítima y prevención de la contaminación por los buques (COSS) y se modifican los reglamentos relativos a la seguridad marítima y a la prevención de la contaminación por los buques (DO L 324 de 29.11.2002, p. 1).

([23]) Reglamento (UE) 2016/1625 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, que modifica el Reglamento (CE) n.º 1406/2002 por el que se crea la Agencia Europea de Seguridad Marítima (DO L 251 de 16.9.2016, p. 77).

Artículo 24

Transposición

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 28 de junio de 2021. Informarán de ello inmediatamente a la Comisión.

Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una 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 25

Entrada en vigor

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

Artículo 26

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

ANEXO 1

REQUISITOS DE LOS PLANES DE RECEPCIÓN Y MANIPULACIÓN DE DESECHOS

Los planes de recepción y manipulación de desechos comprenderán todos los tipos de desechos generados por los buques que visitan normalmente el puerto y se elaborarán en función del tamaño del puerto y de los tipos de buques que hagan escala en él.

Los planes de recepción y manipulación de desechos deberán contener los elementos siguientes:

a) una evaluación de la necesidad de disponer de instalaciones portuarias receptoras, habida cuenta de las necesidades de los buques que visitan normalmente el puerto;

b) una descripción del tipo y la capacidad de las instalaciones portuarias receptoras;

c) una descripción de los procedimientos de recepción y recogida de desechos generados por buques;

d) una descripción del sistema de recuperación de costes;

e) una descripción del procedimiento para comunicar supuestas deficiencias de las instalaciones portuarias receptoras;

f) una descripción del procedimiento de consulta permanente con los usuarios del puerto, contratistas de desechos, operadores de terminales y otras partes interesadas, y

g) una visión de conjunto de los tipos y cantidades de desechos recibidos de buques y manipulados en las instalaciones.

Los planes de recepción y manipulación de desechos podrán incluir:

a) un resumen de la normativa nacional aplicable y el procedimiento y trámites para la entrega de desechos a las instalaciones portuarias receptoras;

b) los datos de un punto de contacto en el puerto;

c) una descripción del equipo y los procesos de tratamiento previo de flujos de desechos específicos en el puerto, en su caso;

d) una descripción de los métodos de registro del uso real de las instalaciones portuarias receptoras;

e) una descripción de los métodos de registro de las cantidades de desechos entregadas por buques;

f) una descripción de los métodos de gestión de los distintos flujos de desechos en el puerto.

Los procedimientos de recepción, recogida, almacenamiento, tratamiento y eliminación deberán ser conformes en todos sus aspectos a un plan de gestión medioambiental adecuado para la progresiva reducción del impacto ambiental de dichas actividades. Se presumirá tal conformidad si los procedimientos se ajustan a lo dispuesto en el Reglamento (CE) n.º 1221/2009 del Parlamento Europeo y del Consejo ([1]).

([1]) Reglamento (CE) n.º 1221/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, relativo a la participación voluntaria de organizaciones en un sistema comunitario de gestión y auditoría medioambientales (EMAS), y por el que se derogan el Reglamento (CE) n.º 761/2001 y las Decisiones 2001/681/CE y 2006/193/CE de la Comisión (DO L 342 de 22.12.2009, p. 1).

ANEXO 2

FORMATO NORMALIZADO DEL FORMULARIO DE NOTIFICACIÓN PREVIA PARA LA ENTREGA DE DESECHOS A INSTALACIONES PORTUARIAS RECEPTORAS

Notificación de la entrega de desechos a: *(nombre del puerto de escala a que se refiere el artículo 6 de la Directiva (UE) 2019/883)*

El presente formulario debe llevarse a bordo del buque junto con el correspondiente Libro de registro de hidrocarburos, Libro de registro de carga, Libro de registro de basuras o plan de gestión de basuras exigidos por el Convenio MARPOL.

1. PORMENORES DEL BUQUE

1.1 Nombre del buque:	1.5 Propietario o armador:
1.2 Número OMI:	1.6 Número o letras distintivas:
	Número de identificación del servicio móvil marítimo (número MMSI):
1.3 Arqueo bruto:	1.7 Estado de abanderamiento:
1.4 Tipo de buque: ☐ Petrolero ☐ Quimiquero ☐ Granelero ☐ Portacontenedores ☐ Buque de carga distinto de los anteriores ☐ Buque de pasaje ☐ Buque de transbordo rodado ☐ Otro (especificar)	

2. PORMENORES DEL PUERTO Y DEL VIAJE

2.1. Nombre de la localidad/terminal:	2.6. Último puerto en el que se entregaron desechos:
2.2. Fecha y hora de la llegada:	2.7. Fecha de la última entrega:
2.3. Fecha y hora de la partida:	2.8. Siguiente puerto de entrega:
2.4. Último puerto y país:	2.9. Persona que presenta este formulario (si es distinta del capitán):
2.5. Siguiente puerto o país (si se conoce):	

3. TIPO Y CANTIDAD DE DESECHOS Y CAPACIDAD DE ALMACENAMIENTO

Tipo	Desechos que van a entregarse (m^3)	Máxima capacidad específica de almacenamiento (m^3)	Cantidad de desechos que quedan a bordo (m^3)	Puerto en el que se van a entregar los desechos restantes	Cantidad estimada de desechos que van a generarse entre la notificación y el siguiente puerto de escala (m^3)
Anexo I del Convenio MARPOL-Hidrocarburos					
Aguas de sentina oleosas					
Residuos oleosos (fangos)					
Aguas oleosas procedentes del lavado de tanques					
Agua de lastre sucia					

Tipo	Desechos que van a entregarse (m^3)	Máxima capacidad específica de almacenamiento (m^3)	Cantidad de desechos que quedan a bordo (m^3)	Puerto en el que se van a entregar los desechos restantes	Cantidad estimada de desechos que van a generarse entre la notificación y el siguiente puerto de escala (m^3)
Depósitos y fangos procedentes de la limpieza de tanques					
Otros (especifíquese)					
Anexo II del Convenio MARPOL-SUSTANCIAS NOCIVAS LÍQUIDAS (1)					
Sustancia de categoría X					
Sustancia de categoría Y					
Sustancia de categoría Z					
Otras sustancias					
Anexo IV del Convenio MARPOL-Aguas sucias					
Anexo V del Convenio MARPOL-Basuras					
A. Plásticos					
B. Desechos de alimentos					
C. Desechos domésticos (por ejemplo, productos de papel, trapos, vidrios, metales, botellas, loza, etc.)					
D. Aceite de cocina					
E. Cenizas de incinerador					
F. Desechos operacionales					
G. Cadáveres de animales					
H. Artes de pesca					
I. Desechos electrónicos					

(1) Indíquese el nombre de expedición correcto de la sustancia nociva líquida en cuestión.

Tipo	Desechos que van a entregarse (m^3)	Máxima capacidad específica de almacenamiento (m^3)	Cantidad de desechos que quedan a bordo (m^3)	Puerto en el que se van a entregar los desechos restantes	Cantidad estimada de desechos que van a generarse entre la notificación y el siguiente puerto de escala (m^3)
J. Residuos de carga (1) nocivos para el medio marino)					
K. Residuos de carga (2) (no nocivos para el medio marino)					
Anexo VI del Convenio MARPOL-Contaminación atmosférica					
Sustancias que agotan la capa de ozono y equipo que contenga tales sustancias (3)					
Residuos de la limpieza de gases de escape					

Otros desechos no regulados en el Convenio MARPOL					
Desechos pescados de manera no intencionada					

Notas

1. Esta información se utilizará a efectos del control por el Estado rector del puerto y otros fines de inspección.
2. Este formulario es de obligado cumplimiento salvo si el buque disfruta de una exención de conformidad con el artículo 9 de la Directiva (UE) 2019/883

(1) Pueden ser estimaciones. Indíquese el nombre de expedición correcto de la carga seca.
(2) Pueden ser estimaciones. Indíquese el nombre de expedición correcto de la carga seca.
(3) Resultantes de las actividades normales de mantenimiento a bordo.

ANEXO 3

FORMATO NORMALIZADO DEL RECIBO DE ENTREGA DE DESECHOS

El representante designado del proveedor de la instalación portuaria receptora deberá facilitar este formulario al capitán del buque que haya entregado desechos de conformidad con el artículo 7 de la Directiva (UE) 2019/883

El presente formulario se llevará a bordo del buque junto con el correspondiente Libro de registro de hidrocarburos, Libro de registro de carga, Libro de registro de basuras o plan de gestión de basuras exigidos por el Convenio MARPOL.

1. PORMENORES DE LA INSTALACIÓN PORTUARIA RECEPTORA Y DEL PUERTO

1.1. Nombre de la localidad/terminal:
1.2. Proveedor(es) de la instalación portuaria receptora:
1.3. Proveedor(es) de la instalación de tratamiento, si difieren de la anterior:
1.4. Fecha y hora de la entrega de desechos: desde: hasta:

2. PORMENORES DEL BUQUE

2.1. Nombre del buque:	2.5. Propietario o armador:
2.2. Número OMI:	2.6. Número o letras distintivas: Número de identificación del servicio móvil marítimo (número MMSI):
2.3. Arqueo bruto:	2.7. Estado de abanderamiento:
2.4. Tipo de buque: ☐ Petrolero ☐ Quimiquero ☐ Granelero ☐ Portacontenedores ☐ Otros buques de carga ☐ Buque de pasaje ☐ Buque de transbordo rodado ☐ Otro (especifíquese)	

3. TIPO Y CANTIDAD ESTIMADA DE DESECHOS RECIBIDOS

Anexo I del Convenio MARPOL-Hidrocarburos	Cantidad (m^3)
Aguas de sentina oleosas	
Residuos oleosos (fangos)	
Aguas oleosas procedentes del lavado de tanques	
Agua de lastre sucia	
Depósitos y fangos procedentes de la limpieza de tanques	
Otros (especifíquese)	
Anexo II del Convenio MARPOL-Sustancias nocivas líquidas	Cantidad (m^3)/Denominación (1)
Sustancia de categoría X	
Sustancia de categoría Y	
Sustancia de categoría Z	
Otras sustancias	
Anexo IV del Convenio MARPOL-Aguas sucias	Cantidad (m^3)

Anexo V del Convenio MARPOL-Basuras	Cantidad (m^3)
A. Plásticos	
B. Desechos de alimentos	
C. Desechos domésticos (por ejemplo, productos de papel, trapos, vidrios, metales, botellas, loza, etc.)	
D. Aceite de cocina	
E. Cenizas del incinerador	
F. Desechos operacionales	
G. Cadáveres de animales	
H. Artes de pesca	
I. Desechos electrónicos	
J. Residuos de carga (2) (nocivos para el medio marino)	
K. Residuos de carga (2) (no nocivos para el medio marino)	
Anexo VI del Convenio MARPOL-Contaminación atmosférica	Cantidad (m^3)
Sustancias que agotan la capa de ozono y equipo que contenga tales sustancias	
Residuos de la limpieza de gases de escape	
Otros desechos no regulados en el Convenio MARPOL	Cantidad (m^3)
Desechos pescados de manera no intencionada	

(1) Indíquese el nombre de expedición correcto de la sustancia nociva líquida en cuestión.
(2) Indíquese el nombre de expedición correcto de la carga seca.

ANEXO 4

CATEGORÍAS DE COSTES Y DE INGRESOS NETOS RELACIONADOS CON LA EXPLOTACIÓN Y GESTIÓN DE LAS INSTALACIONES PORTUARIAS RECEPTORAS

Costes directos	Costes indirectos	Ingresos netos
Costes operativos directos derivados de la entrega efectiva de desechos generados por buques, incluidas las partidas de costes enumeradas a continuación.	Costes administrativos indirectos derivados de la gestión del sistema en el puerto, incluidas las partidas de costes enumeradas a continuación.	Ingresos netos procedentes de los programas para la gestión de desechos y la financiación nacional o regional disponible, incluidos los tipos de ingresos enumerados a continuación.
— Suministro de infraestructuras para las instalaciones portuarias receptoras, incluyendo contenedores, tanques, herramientas de procesamiento, barcazas, camiones, recepción de desechos e instalaciones de tratamiento. — Cánones por arrendamiento financiero del espacio, en su caso, o de los equipos necesarios para las operaciones de las instalaciones portuarias receptoras. — Operaciones efectivas de las instalaciones portuarias receptoras: recogida de los desechos del buque, transporte de los desechos desde las instalaciones portuarias receptoras para su tratamiento final, mantenimiento y limpieza de las instalaciones portuarias receptoras, costes de personal, incluidas las horas extraordinarias, suministro eléctrico, análisis de desechos y seguros. — Preparación para la reutilización, el reciclado o la eliminación finales de desechos generados por buques, incluida su recogida separada. — Administración: facturación, expedición de recibos de entrega de desechos al buque, comunicación de información.	— Elaboración y aprobación del plan de recepción y manipulación de desechos, incluida toda auditoría del plan y su aplicación. — Actualización del plan de recepción y manipulación de desechos, incluidos los costes laborales y de consultoría, en su caso. — Organización de los procedimientos de consulta para la (re)evaluación del plan de recepción y manipulación de desechos. — Gestión de los sistemas de notificación y de recuperación de los costes, que incluye la aplicación de tarifas reducidas a los «buques verdes», la puesta a disposición de sistemas de TI en el puerto y los análisis estadísticos, y los costes laborales correspondientes — Organización de procedimientos de contratación pública para la puesta a disposición de instalaciones portuarias receptoras, así como expedición de las autorizaciones necesarias a tal fin. — Comunicación de información a los usuarios del puerto mediante la distribución de folletos, la colocación de señales y carteles en el puerto o la publicación de la información en el sitio web del puerto, y transmisión electrónica de la información exigida por el artículo 5. — Gestión de los programas de gestión de desechos: regímenes de responsabilidad ampliada del productor, reciclado y solicitud y ejecución de los fondos nacionales o regionales. — Otros costes administrativos: costes de supervisión y notificación electrónica de las exenciones, conforme a lo exigido en el artículo 9.	— Beneficios financieros netos derivados de los regímenes de responsabilidad ampliada del productor. — Otros ingresos netos procedentes de la gestión de desechos, como los regímenes de reciclado. — Financiación en el marco del Fondo Europeo Marítimo y de Pesca (FEMP). — Otros subsidios o financiación a disposición de los puertos en relación con la gestión de desechos y la pesca.

ANEXO 5

CERTIFICADO DE EXENCIÓN EN VIRTUD DEL ARTÍCULO 9 EN RELACIÓN CON LOS REQUISITOS PREVISTOS EN EL ARTÍCULO 6, EL ARTÍCULO 7, APARTADO 1, Y EL ARTÍCULO 8 DE LA DIRECTIVA (UE) 2019/883 EN EL PUERTO O LOS PUERTOS DE [*INSÉRTESE PUERTO*] EN [*INSÉRTESE ESTADO MIEMBRO*] [1]

Nombre del buque	Número o letras distintivas	Estado de abanderamiento
[*Insértese el nombre del buque*]	[*Insértese el número OMI*]	[*Insértese el Estado de abanderamiento*]

opera en tráfico regular, de acuerdo con un horario o una ruta predeterminada, con escalas frecuentes y regulares en el puerto o los puertos siguientes, situados en [*insértese el nombre del Estado miembro*]:

[ ]

y hace escala en estos puertos al menos una vez por quincena:

[ ]

y ha establecido un acuerdo para garantizar el pago de las tarifas y la entrega de los desechos en el puerto, o a un tercero en el puerto de:

[ ]

y, por tanto, está exento, con arreglo al [*insértese la disposición aplicable de la normativa nacional del país*], [*de los requisitos de*:

☐ *entrega obligatoria de desechos generados por buques*,

☐ *notificación previa de los desechos, y*

☐ *pago de la tarifa obligatoria en el/los puerto(s) siguiente(s):]*

El presente certificado será válido hasta el [*insértese la fecha*], salvo que, antes de esa fecha, se modifiquen los motivos por los cuales se expide el certificado.

Lugar y fecha

.....

Nombre
Cargo

[1] Táchese lo que no proceda.

DIRECTIVA (UE) 2019/884 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 82, apartado 1, párrafo segundo, letra d),

Vista la propuesta de la Comisión Europea,

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

De conformidad con el procedimiento legislativo ordinario ([1]),

Considerando lo siguiente:

(1) La Unión se ha fijado el objetivo de ofrecer a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de las personas. Este objetivo debe alcanzarse mediante, entre otras vías, medidas adecuadas para prevenir y combatir la delincuencia, incluida la delincuencia organizada y el terrorismo.

(2) Dicho objetivo exige que la información sobre condenas pronunciadas en los Estados miembros se tenga en cuenta fuera del Estado miembro de condena, tanto en el curso de un nuevo proceso penal, según lo previsto en la Decisión Marco 2008/675/JAI del Consejo ([2]), como para prevenir nuevas infracciones.

(3) Dicho objetivo presupone el intercambio entre las autoridades competentes de los Estados miembros de información extractada de los registros de antecedentes penales. Dicho intercambio de información está organizado y facilitado por las normas recogidas en la Decisión Marco 2009/315/JAI del Consejo ([3]) y por el Sistema Europeo de Información de Antecedentes Penales (ECRIS) establecido por la Decisión 2009/316/JAI del Consejo ([4]).

(4) El marco legal vigente del ECRIS, sin embargo, no aborda suficientemente las particularidades de las solicitudes relacionadas con nacionales de terceros países. Aunque ya es posible intercambiar información sobre nacionales de terceros países a través del ECRIS, no existe ningún procedimiento o mecanismo común de la Unión para hacerlo con eficacia, rapidez y precisión.

(5) Dentro de la Unión, la información sobre nacionales de terceros países no se recoge como se hace con la de los nacionales de los Estados miembros, sino que únicamente se conserva en los Estados miembros en que se hayan impuesto las condenas. Por lo tanto, solo se puede tener una visión completa del historial de antecedentes penales de un nacional de un tercer país si se solicita dicha información a todos los Estados miembros.

(6) Estas solicitudes generales imponen una carga administrativa desproporcionada a todos los Estados miembros, incluidos aquellos que no poseen información sobre ese nacional concreto de un tercer país. En la práctica, dicha carga disuade a los Estados miembros de solicitar a otros Estados miembros información sobre nacionales de terceros países, lo que obstaculiza gravemente el intercambio de información entre Estados miembros y limita su acceso a la información sobre antecedentes penales a la información que se conserva en su propio registro nacional. Como consecuencia de ello, aumenta el riesgo de que el intercambio de información entre Estados miembros sea ineficaz y fragmentario.

([1]) Posición del Parlamento Europeo de 12 de marzo de 2019 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 9 de abril de 2019.

([2]) Decisión Marco 2008/675/JAI del Consejo, de 24 de julio de 2008, relativa a la consideración de las resoluciones condenatorias entre los Estados miembros de la Unión Europea con motivo de un nuevo proceso penal (DO L 220 de 15.8.2008, p. 32).

([3]) Decisión Marco 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L 93 de 7.4.2009, p. 23).

([4]) Decisión 2009/316/JAI del Consejo, de 6 de abril de 2009, por la que se establece el Sistema Europeo de Información de Antecedentes Penales (ECRIS) en aplicación del artículo 11 de la Decisión Marco 2009/315/JAI (DO L 93 de 7.4.2009, p. 33).

(7) Con el fin de mejorar la situación, la Comisión presentó una propuesta, que condujo a la adopción del Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo ([5]) por el que se crea un sistema centralizado en el ámbito de la Unión que contiene los datos personales de los nacionales de terceros países condenados, y permite la identificación de los Estados miembros que posean información relativa a sus condenas anteriores («ECRIS-TCN»).

(8) El ECRIS-TCN permitirá a la autoridad central de un Estado miembro averiguar de forma rápida y eficaz en qué otros Estados miembros hay almacenada información sobre los antecedentes penales de un nacional de un tercer país, de manera que el marco existente del ECRIS pueda utilizarse para solicitar la información sobre los antecedentes penales a dichos Estados miembros, de conformidad con la Decisión Marco 2009/315/JAI.

(9) El intercambio de información sobre condenas penales es importante en cualquier estrategia de lucha contra la delincuencia y el terrorismo. Si los Estados miembros aprovecharan todo el potencial del ECRIS, esto contribuiría a que la justicia penal diese respuesta a la radicalización que conduce al terrorismo y al extremismo violento.

(10) Con el fin de aumentar la utilidad de la información sobre las condenas e inhabilitaciones resultantes de condenas por delitos sexuales contra menores, la Directiva 2011/93/UE del Parlamento Europeo y del Consejo ([6]) establece la obligación de los Estados miembros de adoptar las medidas necesarias para garantizar que, para la contratación de una persona para un puesto que implique un contacto directo y habitual con menores, se transmita la información relativa a la existencia de condenas por delitos sexuales contra menores que consten en el registro de antecedentes penales, así como cualquier inhabilitación que lleven aparejada dichas condenas, de conformidad con los procedimientos establecidos en la Decisión Marco 2009/315/JAI. El propósito de este mecanismo es garantizar que una persona condenada por un delito sexual contra menores no pueda ocultar dicha condena o inhabilitación a fin de ejercer una actividad profesional que conlleve un contacto directo y habitual con menores en otro Estado miembro.

(11) La presente Directiva tiene por objeto introducir en la Decisión Marco 2009/315/JAI las modificaciones necesarias para permitir un intercambio eficaz de información sobre las condenas de nacionales de terceros países por medio del ECRIS. Obliga a los Estados miembros a adoptar las medidas necesarias para garantizar que las condenas vayan acompañadas de información sobre la nacionalidad o nacionalidades del condenado, siempre que los Estados miembros dispongan de dicha información. Asimismo, introduce procedimientos para responder a las solicitudes de información, garantiza que los extractos de antecedentes penales solicitados por un nacional de un tercer país se complementen con información de otros Estados miembros, y dispone los cambios técnicos necesarios para que el sistema de intercambio de información funcione.

(12) La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([7]) debe aplicarse al tratamiento de los datos personales por parte de las autoridades nacionales competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([8]) debe aplicarse al tratamiento de datos personales por parte de las autoridades nacionales, siempre que dicho tratamiento no entre en el ámbito de aplicación de la Directiva (UE) 2016/680.

(13) A fin de garantizar condiciones uniformes para la aplicación de la Decisión Marco 2009/315/JAI, deben incorporarse a dicha Decisión Marco los principios de la Decisión 2009/316/JAI, y conferirse competencias de ejecución a la Comisión. Dichas competencias deben ejercerse de conformidad con lo dispuesto en el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([9]).

([5]) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas («ECRIS-TCN») a fin de complementar el Sistema Europeo de Información de Antecedentes Penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

([6]) Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo (DO L 335 de 17.12.2011, p. 1).

([7]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

([8]) 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).

([9]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(14) La infraestructura de comunicación común utilizada para el intercambio de información de antecedentes penales debe ser la Red de servicios transeuropeos seguros de telemática entre administraciones (sTESTA), cualquier otro desarrollo de la misma o cualquier otra red segura alternativa.

(15) Con independencia de la posibilidad de usar los programas financieros de la Unión de acuerdo con las normas aplicables, cada Estado miembro debe correr con sus propios costes derivados de la aplicación, la administración, el uso y el mantenimiento de su base de datos de antecedentes penales, así como de la aplicación, la administración, el uso y el mantenimiento de las adaptaciones técnicas necesarias para poder usar el ECRIS.

(16) La presente Directiva respeta los derechos y libertades fundamentales reconocidos en particular en la Carta de los Derechos Fundamentales de la Unión Europea, incluido el derecho a la protección de los datos de carácter personal, el derecho a un recurso judicial y administrativo, el principio de igualdad ante la ley, el derecho a un juicio justo, la presunción de inocencia y la prohibición general de discriminación. La presente Directiva debe aplicarse de conformidad con estos derechos y principios.

(17) Dado que el objetivo de la presente Directiva, a saber, posibilitar el intercambio rápido y eficiente de información precisa de antecedentes penales de nacionales de terceros países, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, mediante la puesta en marcha de normas comunes, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dicho objetivo.

(18) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al Tratado de Funcionamiento de la Unión Europea (TFUE), Dinamarca no participa en la adopción de la presente Directiva y no queda vinculada por esta ni sujeta a su aplicación.

(19) De conformidad con los artículos 1 y 2, y con el artículo 4 *bis*, apartado 1, del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al TUE y al TFUE, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda no participa en la adopción de la presente Directiva y no queda vinculada por ella ni sujeta a su aplicación.

(20) De conformidad con el artículo 3 y el artículo 4 *bis*, apartado 1, del Protocolo n.º 21, el Reino Unido ha notificado su deseo de participar en la adopción y aplicación de la presente Directiva.

(21) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([10]), emitió un dictamen el 13 de abril de 2016 ([11]).

(22) Procede, por tanto, modificar la Decisión Marco 2009/315/JAI en consecuencia.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Modificaciones de la Decisión Marco 2009/315/JAI

La Decisión Marco 2009/315/JAI se modifica como sigue:

1) El artículo 1 se sustituye por el texto siguiente:

«*Artículo 1*

Objeto

La presente Decisión Marco:

a) define las condiciones en las que un Estado miembro de condena comparte con otros Estados miembros información sobre condenas;

([10]) 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).

([11]) DO C 186 de 25.5.2016, p. 7.

b) define las obligaciones del Estado miembro de condena y del Estado miembro de nacionalidad de la persona condenada (en lo sucesivo, "Estado miembro de nacionalidad de la persona"), y especifica los métodos que se han de seguir para responder a una solicitud de información extractada de registros de antecedentes penales;

c) establece un sistema descentralizado de tecnología de la información para el intercambio de información sobre condenas basado en las bases de datos de antecedentes penales de cada Estado miembro, el Sistema Europeo de Información de Antecedentes Penales (ECRIS).».

2) En el artículo 2 se añaden las letras siguientes:

«d) "Estado miembro de condena": el Estado miembro en el que se pronuncia una condena;

e) "nacional de un tercer país": una persona que no es ciudadano de la Unión en el sentido del artículo 20, apartado 1, del TFUE, o que es apátrida o de nacionalidad desconocida;

f) "datos dactiloscópicos": los datos relativos a las impresiones simples y roladas de las huellas dactilares de cada uno de los dedos de una persona;

g) "imagen facial": una imagen digital del rostro de una persona;

h) "aplicación de referencia ECRIS": los programas elaborados por la Comisión y puestos a disposición de los Estados miembros para el intercambio de información sobre los registros de antecedentes penales a través del ECRIS.».

3) En el artículo 4, el apartado 1 se sustituye por el texto siguiente:

«1. Cada Estado miembro de condena adoptará todas las medidas necesarias para garantizar que las condenas pronunciadas en su territorio vayan acompañadas de información sobre la nacionalidad o nacionalidades de la persona condenada, si esta es nacional de otro Estado miembro o nacional de un tercer país. En caso de que el condenado sea de nacionalidad desconocida o apátrida, el registro de antecedentes penales reflejará esta circunstancia.».

4) El artículo 6, se modifica como sigue:

a) el apartado 3 se sustituye por el texto siguiente:

«3. Cuando un nacional de un Estado miembro solicite a la autoridad central de otro Estado miembro información sobre sus propios antecedentes penales, dicha autoridad central remitirá a la autoridad central del Estado miembro de nacionalidad de la persona una solicitud de información y datos conexos en extracto de sus antecedentes penales, e incluirá dicha información y datos conexos en el extracto que se facilite a la persona de que se trate.»;

b) se añade el apartado siguiente:

«3 *bis*. Si un nacional de un tercer país solicita a la autoridad central de un Estado miembro información sobre sus propios antecedentes penales, dicha autoridad central solamente remitirá a las autoridades centrales de los Estados miembros que conserven información de los antecedentes penales de dicha persona una solicitud de información y datos conexos en extracto de sus antecedentes penales e incluirá dicha información y datos conexos en el extracto que se facilite a la persona de que se trate.».

5) El artículo 7 se modifica como sigue:

a) el apartado 4 se sustituye por el texto siguiente:

«4. Si, en virtud de lo dispuesto en el artículo 6, se solicita a la autoridad central de un Estado miembro que no sea el de nacionalidad de la persona información extractada del registro de antecedentes penales sobre condenas pronunciadas contra un nacional de un Estado miembro, el Estado miembro requerido transmitirá dicha información en las mismas condiciones que las previstas en el artículo 13 del Convenio Europeo de Asistencia Judicial en Materia Penal.»;

b) se añade el apartado siguiente:

«4 *bis*. Si, en virtud de lo dispuesto en el artículo 6, se solicita para un proceso penal información extractada del registro de antecedentes penales sobre condenas pronunciadas contra un nacional de un tercer país, el Estado miembro requerido transmitirá la información sobre las condenas pronunciadas en su territorio e inscritas en el registro de antecedentes penales y sobre las condenas pronunciadas en terceros países y posteriormente transmitidas e inscritas en el registro de antecedentes penales.

Si dicha información se solicita para un fin distinto de un proceso penal, se aplicará lo dispuesto en el apartado 2 del presente artículo.».

6) En el artículo 8, el apartado 2 se sustituye por el texto siguiente:

«2. Las respuestas a las solicitudes contempladas en el artículo 6, apartados 2, 3 y 3 *bis*, se transmitirán en un plazo de veinte días hábiles a partir de la fecha de recepción de la solicitud.».

7) El artículo 9 se modifica como sigue:

a) en el apartado 1, los términos «artículo 7, apartados 1 y 4» se sustituyen por «artículo 7, apartados 1, 4 y 4 *bis*»;

b) en el apartado 2, los términos «artículo 7, apartados 2 y 4» se sustituyen por «artículo 7, apartados 2, 4 y 4 *bis*»;

c) en el apartado 3, los términos «artículo 7, apartados 1, 2 y 4» se sustituyen por «artículo 7, apartados 1, 2, 4 y 4 *bis*».

8) El artículo 11 se modifica como sigue:

a) en el apartado 1, párrafo primero, letra c), se añade el inciso siguiente:

«iv) imagen facial.»;

b) los apartados 3 a 7 se sustituyen por el texto siguiente:

«3. Las autoridades centrales de los Estados miembros transmitirán la siguiente información por vía electrónica, utilizando el ECRIS y un formato normalizado de conformidad con las normas que se establezcan en los actos de ejecución:

a) información contemplada en el artículo 4;

b) las solicitudes contempladas en el artículo 6;

c) las respuestas contempladas en el artículo 7, y

d) otra información pertinente.

4. Si el modo de transmisión a que se refiere el apartado 3 no está disponible, las autoridades centrales de los Estados miembros transmitirán toda la información contemplada en el apartado 3 a través de cualquier medio capaz de generar un registro escrito en condiciones que permitan a la autoridad central del Estado miembro receptor verificar la autenticidad de la información, tomando en consideración la seguridad de la transmisión.

Si el modo de transmisión a que se refiere el apartado 3 no está disponible durante un período de tiempo prolongado, el Estado miembro de que se trate informará de ello a los demás Estados miembros y a la Comisión.

5. Cada Estado miembro realizará las modificaciones técnicas necesarias para poder usar el formato normalizado, a fin de transmitir por vía electrónica toda la información contemplada en el apartado 3 a otros Estados miembros a través del ECRIS. Cada Estado miembro notificará a la Comisión la fecha a partir de la cual podrá llevar a cabo dichas transmisiones.».

9) Se insertan los artículos siguientes:

«*Artículo 11* bis

Sistema Europeo de Información de Antecedentes Penales (ECRIS)

1. Para intercambiar información extractada de registros de antecedentes penales por vía electrónica de conformidad con la presente Decisión Marco, se establece un sistema descentralizado de tecnología de la información basado en las bases de datos de antecedentes penales de cada Estado miembro, el Sistema Electrónico de Información de Antecedentes Penales (ECRIS). Este sistema estará compuesto por los siguientes elementos:

a) aplicación de referencia ECRIS;

b) una infraestructura de comunicación común entre las autoridades centrales que proporcione una red cifrada.

Para garantizar la confidencialidad y la integridad de la información de los registros de antecedentes penales transmitida a otros Estados miembros, se aplicarán las medidas técnicas y organizativas oportunas, teniendo en cuenta los últimos adelantos de la técnica, el coste de la ejecución y los riesgos que plantea el tratamiento de la información.

2. Todos los datos de los registros de antecedentes penales se almacenarán únicamente en bases de datos gestionadas por los Estados miembros.

3. Las autoridades centrales de los Estados miembros no tendrán acceso directo a las bases de datos de los registros de antecedentes penales de otros Estados miembros.

4. La aplicación de referencia ECRIS y las bases de datos que almacenen, envíen y reciban información extractada de los registros de antecedentes penales funcionarán bajo la responsabilidad del Estado miembro de que se trate. La Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), creada por el Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo (*), dará apoyo a los Estados miembros conforme a las funciones que le atribuye el Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo (**)

5. La infraestructura de comunicación común será gestionada bajo la responsabilidad de la Comisión. Cumplirá los necesarios requisitos de seguridad y responderá plenamente a las necesidades del ECRIS.

6. La agencia eu-LISA facilitará, proseguirá el desarrollo y mantendrá la aplicación de referencia ECRIS.

7. Cada Estado miembro sufragará sus propios gastos derivados de la aplicación, administración, uso y mantenimiento de su base de datos de antecedentes penales y la instalación y uso de la aplicación de referencia ECRIS.

La Comisión sufragará los costes derivados de la aplicación, administración, uso, mantenimiento y desarrollo futuro de la infraestructura de comunicación común.

8. Los Estados miembros que utilicen su propia aplicación nacional ECRIS de conformidad con lo dispuesto en el artículo 4, apartados 4 a 8, del Reglamento(UE) 2019/816 podrán seguir utilizando su propia aplicación nacional ECRIS en lugar de la aplicación de referencia ECRIS, siempre que cumplan todas las condiciones que se establecen en dichos apartados.

Artículo 11 ter

Actos de ejecución

1. La Comisión establecerá las medidas siguientes mediante actos de ejecución:

a) el formato normalizado contemplado en el artículo 11, apartado 3, incluido lo referente a la información sobre el delito que dio lugar a la condena y a la información sobre el contenido de la condena;

b) las normas relativas a la aplicación técnica del ECRIS y el intercambio de datos dactiloscópicos;

c) cualquier otro medio técnico para organizar y facilitar intercambios de información sobre condenas entre las autoridades centrales de los Estados miembros, en particular:

i) los medios para facilitar la comprensión y la traducción automática de la información transmitida,

ii) los medios para el intercambio por vía electrónica de la información, en especial la relativa a las normas técnicas que deberán utilizarse y, en su caso, los procedimientos de intercambio aplicables.

2. Los actos de ejecución a que se refiere el apartado 1 del presente artículo se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 12 *bis*, apartado 2.

(*) Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n.º 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n.º 1077/2011 (DO L 295 de 21.11.2018, p. 99).

(**) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas ("ECRIS-TCN") a fin de complementar el Sistema Europeo de Información de Antecedentes Penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).»

10) Se inserta el artículo siguiente:

«*Artículo 12* bis

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, será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Si el comité no emite un dictamen, la Comisión no adoptará el proyecto de acto de ejecución y se aplicará el artículo 5, apartado 4, párrafo tercero, del Reglamento (UE) n.º 182/2011.».

11) Se inserta el artículo siguiente:

«*Artículo 13* bis

Información por parte de la Comisión y revisión

1. A más tardar el 29 de junio de 2023, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la aplicación de la presente Decisión Marco. El informe evaluará en qué medida los Estados miembros han adoptado las medidas necesarias para cumplir con la presente Decisión Marco, incluida su ejecución técnica.

2. El informe irá acompañado, en su caso, de las correspondientes propuestas legislativas.

3. La Comisión publicará periódicamente un informe sobre el intercambio de información extractada de los registros de antecedentes penales a través del ECRIS y en relación con el uso del ECRIS-TCN, basado en particular en las estadísticas facilitadas por eu-LISA y por los Estados miembros de conformidad con el Reglamento (UE) 2019/816. El informe se publicará por primera vez un año después de la presentación del informe contemplado en el apartado 1.

4. El informe de la Comisión contemplado en el apartado 3 abordará en particular el nivel de intercambio de información entre Estados miembros, incluida la relativa a nacionales de terceros países, así como la finalidad de las solicitudes y su número respectivo, incluidas las solicitudes con fines distintos de los procesos penales, como por ejemplo las comprobaciones de antecedentes y las solicitudes de información formuladas por las personas interesadas con respecto a sus propios antecedentes penales.».

Artículo 2

Sustitución de la Decisión 2009/316/JAI

La Decisión 2009/316/JAI queda sustituida en lo que respecta a los Estados miembros vinculados por la presente Directiva, sin perjuicio de las obligaciones de dichos Estados miembros con respecto a la fecha de aplicación de dicha Decisión.

Artículo 3

Transposición

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 28 de junio de 2022. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Incluirán igualmente una mención en la que se precise que las referencias hechas, en las disposiciones legales, reglamentarias y administrativas vigentes, a la Decisión sustituida por la presente Directiva se entenderán hechas a la presente Directiva. 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.

3. Los Estados miembros llevarán a cabo las modificaciones técnicas previstas en el artículo 11, apartado 5, de la Decisión Marco 2009/315/JAI, tal y como ha sido modificada por la presente Directiva, a más tardar el 28 de junio de 2022.

Artículo 4

Entrada en vigor y aplicación

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

El artículo 2 se aplicará a partir del 28 de junio de 2022.

Artículo 5

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros de conformidad con los Tratados.

Hecho en Estrasburgo, el 17 de abril de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA

ISSN 1977-0685 (edición electrónica)
ISSN 1725-2512 (edición papel)

Oficina de Publicaciones de la Unión Europea
2985 Luxemburgo
LUXEMBURGO

ES