COMISIÓN
EUROPEA

Bruselas, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

(Texto pertinente a efectos del EEE)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente propuesta forma parte de un paquete de medidas destinadas a seguir mejorando la resiliencia y las capacidades de respuesta a incidentes de las entidades públicas y privadas, las autoridades competentes y la Unión en su conjunto en el ámbito de la ciberseguridad y la protección de las infraestructuras críticas. Se ajusta a las prioridades fijadas por la Comisión de lograr una Europa adaptada a la era digital y de construir una economía con visión de futuro al servicio de las personas. La ciberseguridad es una de las prioridades de la respuesta de la Comisión a la crisis de la COVID-19. El paquete incluye una nueva Estrategia de Ciberseguridad cuyo objetivo es reforzar la autonomía estratégica de la Unión a fin de mejorar su resiliencia y respuesta colectiva, y de forjar una internet abierta y global. Por último, el paquete comprende una propuesta de directiva sobre la resiliencia de los operadores críticos de servicios esenciales, con la que se persigue reducir las amenazas físicas contra dichos operadores.

La presente propuesta se basa en la Directiva (UE) 2016/1148 relativa a la seguridad de las redes y sistemas de información (Directiva SRI), que constituye el primer acto legislativo a escala de la UE en materia de ciberseguridad y contempla medidas legales para impulsar el nivel global de ciberseguridad en la Unión, y la deroga. La Directiva SRI (1) ha contribuido a mejorar las capacidades en materia de ciberseguridad a nivel nacional al obligar a los Estados miembros a adoptar estrategias nacionales de ciberseguridad y a designar autoridades de ciberseguridad, (2) ha incrementado la cooperación entre los Estados miembros a nivel de la Unión gracias a la creación de diversos foros para facilitar el intercambio de información estratégica y operativa, y (3) ha mejorado la ciberresiliencia de las entidades públicas y privadas de siete sectores específicos (energía, transporte, banca, infraestructuras de los mercados financieros, sanidad, suministro y distribución de agua potable, e infraestructuras digitales) y transversalmente en tres servicios digitales (mercados en línea, motores de búsqueda en línea y servicios de computación en nube) exigiendo a los Estados miembros que garanticen que los operadores de servicios esenciales y los proveedores de servicios digitales cuenten con requisitos en materia de ciberseguridad y notifiquen los incidentes.

La propuesta contribuye a modernizar el marco jurídico vigente al tener en cuenta el aumento de la digitalización del mercado interior en los últimos años y la evolución del panorama de amenazas para la ciberseguridad. Ambas circunstancias se han visto agravadas con el inicio de la crisis de la COVID-19. Asimismo, la propuesta aborda varias deficiencias que impedían aprovechar todo el potencial de la Directiva SRI.

Aunque los logros conseguidos con la Directiva han sido notables y con ella se sentaron las bases de un cambio de mentalidad significativo, también ha demostrado sus limitaciones por lo que respecta a la estrategia institucional y reglamentaria que muchos Estados miembros han aplicado a la ciberseguridad. La transformación digital de la sociedad (agudizada por la crisis de la COVID-19) ha ampliado el panorama de amenazas e introduce nuevos desafíos que exigen respuestas adaptadas e innovadoras. El número de ciberataques continúa aumentando y los ataques son cada vez más sofisticados y proceden de un amplio abanico de fuentes de dentro y fuera de la UE.

En la evaluación del funcionamiento de la Directiva SRI que se llevó a cabo a efectos de la evaluación de impacto se determinaron los siguientes problemas: 1) el bajo nivel de ciberresiliencia de las empresas que operan en la UE; 2) la incoherencia en términos de resiliencia entre Estados miembros y sectores; y 3) el escaso nivel de conciencia situacional

conjunta y la ausencia de una respuesta conjunta en caso de crisis. Por ejemplo, determinados hospitales importantes de un Estado miembro no están incluidos en el ámbito de aplicación de la Directiva SRI y, por ende, no están obligados a aplicar las correspondientes medidas de seguridad, mientras que en otro Estado miembro prácticamente todos los proveedores de asistencia sanitaria del país están cubiertos por los requisitos de seguridad de la Directiva.

Dado que la propuesta es una iniciativa que se enmarca en el programa de adecuación y eficacia de la reglamentación (REFIT), aspira a reducir la carga normativa para las autoridades competentes y los costes de conformidad para las entidades públicas y privadas. Ello se consigue, principalmente, mediante la eliminación de la obligación de que las autoridades competentes identifiquen a los operadores de servicios esenciales y el aumento del nivel de armonización de los requisitos de seguridad y notificación para facilitar el cumplimiento de la normativa por parte de las entidades que prestan servicios transfronterizos. Al mismo tiempo, las autoridades competentes también tendrán que encargarse de varias tareas nuevas, entre ellas la supervisión de entidades pertenecientes a sectores a los que hasta la fecha no se aplicaba la Directiva SRI.

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

La presente propuesta forma parte de un conjunto más amplio de instrumentos jurídicos existentes y futuras iniciativas emprendidas desde la Unión con el objetivo de incrementar la resiliencia de las entidades públicas y privadas frente a las amenazas.

En el ámbito de la ciberseguridad, se trata, en particular, de la Directiva (UE) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (cuyas disposiciones relacionadas con la ciberseguridad se sustituirán por las disposiciones de la propuesta que nos ocupa) y la propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero [COM(2020) 595 final], que tendrá consideración de *lex specialis* con respecto a la presente propuesta en cuanto ambos actos entren en vigor.

Por lo que se refiere a la seguridad física, la propuesta complementa la propuesta de Directiva sobre la resiliencia de las entidades críticas, que revisa la Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (Directiva ICE), en la que se establece un proceso de la Unión para identificar y designar las infraestructuras críticas europeas y un planteamiento para mejorar su protección. En julio de 2020, la Comisión adoptó la Estrategia de la UE para una Unión de la Seguridad[1], en la que se reconocía la mayor interconexión e interdependencia entre las infraestructuras físicas y las digitales. Puso de manifiesto la necesidad de un enfoque más coherente y uniforme entre la Directiva ICE y la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

En consecuencia, la propuesta es acorde con la propuesta de Directiva sobre la resiliencia de las entidades críticas, cuyo objetivo es reforzar la resiliencia de las entidades críticas frente a las amenazas en un gran número de sectores. La finalidad de la propuesta es garantizar que las autoridades competentes, al amparo de ambos actos jurídicos, adopten medidas complementarias e intercambien información según proceda en materia de ciberresiliencia y resiliencia en general, y que los operadores especialmente críticos de los sectores que se consideran «esenciales» en virtud de la presente propuesta también estén sujetos a

[1] COM(2020) 605 final.

obligaciones más generales destinadas a reforzar la resiliencia, haciendo hincapié en los riesgos que no sean cibernéticos.

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

Como se recoge en la Comunicación «Configurar el futuro digital de Europa»[2], es crucial que Europa aproveche todas las ventajas de la era digital y refuerce su industria y capacidad de innovación, dentro de unos límites seguros y éticos. La Estrategia Europea de Datos establece cuatro pilares como requisitos previos esenciales para una sociedad empoderada por el uso de los datos, a saber, la protección de datos, los derechos fundamentales, la seguridad y la ciberseguridad.

En una Resolución de 12 de marzo de 2019, el Parlamento Europeo pidió «a la Comisión que [evaluase] la necesidad de ampliar el ámbito de aplicación de la Directiva SRI a otros sectores y servicios críticos que no están cubiertos por una legislación específica»[3]. El Consejo, en sus Conclusiones de 9 de junio de 2020, celebró «los planes de la Comisión destinados a garantizar unas normas coherentes para los operadores del mercado y facilitar un intercambio de información seguro, sólido y adecuado sobre amenazas e incidentes —en particular, mediante la revisión de la Directiva relativa a la seguridad de las redes y sistemas de información en la Unión (Directiva SRI)— con el fin de encontrar soluciones que puedan mejorar la ciberresiliencia y dar una respuesta más eficaz frente a los ciberataques, en especial en el contexto de las actividades económicas y sociales esenciales, al tiempo que se respetan las competencias de los Estados miembros, en particular la responsabilidad de su seguridad nacional»[4]. Por otro lado, el acto jurídico propuesto debe entenderse sin perjuicio de la aplicación de las normas sobre competencia establecidas en el Tratado de Funcionamiento de la Unión Europea (TFUE).

Habida cuenta de que una parte considerable de las amenazas de ciberseguridad provienen de fuera de la UE, se precisa un enfoque coherente respecto de la cooperación internacional. La presente Directiva constituirá un modelo de referencia que debe promoverse en el contexto de la cooperación de la UE con terceros países, en particular a la hora de prestar asistencia técnica externa.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- **Base jurídica**

La base jurídica de la Directiva SRI es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), cuyo objetivo es el establecimiento y el funcionamiento del mercado interior mediante el refuerzo de las medidas destinadas a la aproximación de las normas nacionales. Como sostuvo el Tribunal de Justicia de la Unión Europea en su sentencia correspondiente al asunto C-58/08, Vodafone y otros, el recurso al artículo 114 del TFUE está justificado cuando existen diferencias entre normas nacionales que tienen un efecto directo sobre el funcionamiento del mercado interior. Igualmente, el Tribunal dictaminó que, cuando un acto basado en el artículo 114 del TFUE ya ha suprimido todos los obstáculos a los intercambios en el ámbito que armoniza, el legislador de la Unión no puede ser privado de la

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_ES.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/es/pdf.

posibilidad de adaptar ese acto a cualquier modificación de las circunstancias o cualquier evolución de los conocimientos, habida cuenta de la tarea que le incumbe de velar por que se protejan los intereses generales reconocidos por el Tratado. Por último, el Tribunal concluyó que las medidas relativas a la aproximación amparadas por el artículo 114 del TFUE están destinadas a conferir un margen de discrecionalidad, en función del contexto general y de las circunstancias específicas de la materia que deba armonizarse en cuanto a la técnica de aproximación más adecuada para lograr el resultado deseado. El acto jurídico propuesto eliminaría los obstáculos al mercado interior y mejoraría su establecimiento y funcionamiento para las entidades esenciales e importantes al establecer normas claras de aplicación general sobre el ámbito de aplicación de la Directiva SRI y armonizar las normas aplicables en el ámbito de la gestión de riesgos de ciberseguridad y notificación de incidentes. Las disparidades que existen actualmente en este ámbito, tanto a nivel legislativo y de supervisión como a escala nacional y de la UE, constituyen obstáculos al mercado interior, ya que las entidades que desarrollan actividades transfronterizas se enfrentan a requisitos normativos diferentes y que posiblemente se solapan o que se aplican de manera distinta, en detrimento del ejercicio de sus libertades de establecimiento y de prestación de servicios. Las diferencias normativas también repercuten negativamente en las condiciones de competencia en el mercado interior por lo que respecta a las entidades del mismo tipo en Estados miembros diferentes.

- **Subsidiariedad (en el caso de competencia no exclusiva)**

La resiliencia en términos de ciberseguridad en toda la Unión no puede ser eficaz si se aplican distintos enfoques de carácter nacional o regional. La Directiva SRI solucionó en parte esta deficiencia al establecer un marco para la seguridad de las redes y sistemas de información a escala nacional y de la Unión. No obstante, su transposición y aplicación también pusieron de manifiesto las deficiencias y limitaciones inherentes de determinadas disposiciones o planteamientos, como por ejemplo la delimitación ambigua del ámbito de aplicación de la Directiva, lo que se tradujo en diferencias significativas en cuanto a la amplitud y la profundidad de la intervención *de facto* de la UE a escala de los Estados miembros. Por otro lado, desde el estallido de la crisis de la COVID-19, la dependencia de la economía europea de las redes y sistemas de información ha aumentado hasta niveles sin precedentes, y los sectores y servicios están cada vez más interconectados. Los siguientes motivos justifican que la intervención de la UE trascienda las medidas actuales de la Directiva SRI: i) la dimensión transfronteriza cada vez más pronunciada de las amenazas y desafíos asociados a las redes y los sistemas de información; ii) el potencial de que la intervención de la Unión mejore unas políticas nacionales efectivas y coordinadas y las facilite; y iii) la contribución de unas acciones políticas concertadas y colaborativas a la protección efectiva de los datos y la privacidad.

- **Proporcionalidad**

Las normas propuestas en la presente Directiva no rebasan los límites estrictamente necesarios para lograr los objetivos específicos de manera satisfactoria. La armonización y racionalización previstas de las medidas de seguridad y las obligaciones de notificación atienden a las peticiones de los Estados miembros y de las empresas de mejorar el marco vigente.

La propuesta tiene en cuenta las prácticas ya existentes en los Estados miembros. Reforzar el nivel de protección conseguido a través de tales requisitos racionalizados y coordinados es proporcionado a los riesgos cada vez mayores que se presentan, en particular aquellos con una

dimensión transfronteriza; son razonables y, en términos generales, se corresponde con el interés de las entidades implicadas de garantizar la continuidad y calidad de sus servicios. Los costes de garantizar una cooperación sistemática entre los Estados miembros serían reducidos en comparación con los daños y perjuicios económicos y sociales causados por los incidentes de ciberseguridad. Por otro lado, las consultas con las partes interesadas organizadas en el contexto de la revisión de la Directiva SRI, incluidos los resultados de la consulta pública y las encuestas específicas, demuestran que la revisión de la Directiva siguiendo las líneas planteadas anteriormente cuenta con apoyo.

- **Elección del instrumento**

La propuesta racionalizará en mayor medida las obligaciones impuestas a las empresas y garantizará un mayor nivel de armonización de dichas obligaciones. Al mismo tiempo, la propuesta tiene por objeto conceder a los Estados miembros la flexibilidad necesaria para tener en cuenta las especificidades nacionales (como, por ejemplo, la posibilidad de identificar entidades esenciales o importantes adicionales más allá del nivel de referencia fijado por el acto jurídico). En consecuencia, procede que el futuro instrumento jurídico sea una directiva, ya que permite mejorar la armonización de manera focalizada y concede cierto grado de flexibilidad a las autoridades competentes.

3. RESULTADOS DE LAS EVALUACIONES *A POSTERIORI*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *a posteriori*/controles de la adecuación de la legislación existente**

La Comisión ha llevado a cabo una evaluación del funcionamiento de la Directiva SRI[5], en la que se ha analizado su pertinencia, valor añadido de la UE, coherencia, eficacia y eficiencia. Las principales constataciones de este análisis son:

- El ámbito de aplicación de la Directiva SRI es excesivamente restringido por lo que respecta a los sectores amparados, principalmente por el incremento de la digitalización en los últimos años y un mayor grado de interconexión, y porque el ámbito de aplicación de la Directiva SRI ya no refleja todos los sectores digitalizados que prestan servicios fundamentales para la economía y la sociedad en su conjunto.
- La Directiva SRI no es suficientemente clara por lo que respecta al ámbito de aplicación para los operadores de servicios esenciales y sus disposiciones no ofrecen suficiente claridad en relación con la competencia nacional sobre los proveedores de servicios digitales, lo que ha dado lugar a que determinados tipos de entidades no hayan sido identificadas en todos los Estados miembros y, en consecuencia, no estén obligadas a implantar medidas de seguridad y a notificar los incidentes.
- La Directiva SRI concedía un amplio margen discrecional a los Estados miembros a la hora de establecer los requisitos de seguridad y de notificación de incidentes aplicables a los operadores de servicios esenciales (OSE). La evaluación muestra que, en algunas situaciones los Estados miembros han aplicado estos requisitos de formas sensiblemente distintas, lo que crea una carga adicional para las empresas que operan en más de un Estado miembro.

[5] [anexo 5 de la evaluación de impacto]

- El régimen de supervisión y ejecución de la Directiva SRI resulta ineficaz. Por ejemplo, los Estados miembros han sido muy reacios a imponer sanciones a las entidades que no contaban con requisitos de seguridad o no notificaban los incidentes. Esta manera de proceder puede tener consecuencias negativas para la ciberresiliencia de entidades individuales.
- Los recursos financieros y humanos destinados por los Estados miembros al cumplimiento de sus tareas (como, por ejemplo, la identificación o supervisión de OSE) y, en consecuencia, los distintos niveles de madurez a la hora de hacer frente a los riesgos de ciberseguridad, varían enormemente, circunstancias que acentúan más si cabe las diferencias en términos de ciberresiliencia entre los Estados miembros.
- Los Estados miembros no comparten información sistemáticamente entre ellos, lo que tiene consecuencias negativas, especialmente para la eficacia de las medidas de ciberseguridad y para el grado de conciencia situacional conjunta a escala de la UE. Lo mismo puede decirse del intercambio de información entre entidades privadas y del compromiso entre las estructuras de cooperación a escala de la UE y las entidades privadas.

- **Consultas con las partes interesadas**

La Comisión ha consultado con un amplio abanico de partes interesadas. Se invitó a los Estados miembros y a las partes interesadas a participar en la consulta pública y en las encuestas y talleres organizados por Wavestone, CEPS e ICF, contratados por la Comisión para llevar a cabo un estudio en apoyo de la revisión de la Directiva SRI. Entre las partes interesadas consultadas había autoridades competentes, órganos de la Unión cuyo trabajo se enmarca en el ámbito de la ciberseguridad, operadores de servicios esenciales, proveedores de servicios digitales, entidades que prestan servicios excluidos del ámbito de aplicación de la Directiva SRI vigente, asociaciones comerciales y organizaciones de consumidores, así como ciudadanos.

Por otro lado, la Comisión ha estado en permanente contacto con las autoridades competentes responsables de la aplicación de la Directiva SRI. El Grupo de Cooperación ha cubierto ampliamente diversos aspectos transversales y sectoriales relacionados con la aplicación. Por último, durante las visitas realizadas en 2019 y 2020 a distintos países en el contexto de la SRI, la Comisión se ha entrevistado con 154 entidades públicas y privadas, así como con 117 autoridades competentes.

- **Obtención y uso de asesoramiento especializado**

La Comisión ha contratado a un consorcio formado por Wavestone, CEPS e ICF para que la ayude con la revisión de la Directiva SRI[6]. El contratista no solo ha recabado el punto de vista de las partes interesadas afectadas directamente por la Directiva SRI a través de encuestas específicas y talleres, sino que también ha consultado a un amplio abanico de expertos en el ámbito de la ciberseguridad, como, por ejemplo, investigadores y profesionales del sector.

[6] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N.º 2020-665. Wavestone, CEPS e ICF.

- **Evaluación de impacto**

La presente propuesta va acompañada de una evaluación de impacto[7] que se remitió al Comité de Control Reglamentario el 23 de octubre de 2020 y recibió un dictamen favorable con observaciones de dicho Comité el 20 de noviembre de 2020. El Comité de Control Reglamentario recomendó algunas mejoras en ciertas partes con el objetivo de: 1) reflejar mejor el papel de las externalidades transfronterizas en el análisis del problema; 2) explicar mejor cómo se cuantificaría el éxito de la iniciativa; 3) justificar en mayor detalle la lista de opciones existentes; 4) detallar en profundidad los costes de las medidas propuestas. La evaluación de impacto se ajustó para responder a estas recomendaciones, así como a las observaciones más detalladas del Comité de Control Reglamentario. Ahora incluye explicaciones más detalladas del papel de las externalidades transfronterizas en el ámbito de la ciberseguridad, un panorama más claro de la forma de medir el éxito, una explicación más detallada del diseño y la lógica que subyace a las distintas opciones y las medidas analizadas dentro de dichas opciones, una explicación más detallada de los aspectos analizados en relación con el ámbito de aplicación sectorial de la Directiva SRI, y precisiones adicionales respecto a los costes.

La Comisión estudió varias opciones para mejorar el marco jurídico en el ámbito de la ciberresiliencia y la respuesta a incidentes:

- «No actuar»: la Directiva SRI se mantendría inalterada y no se adoptaría ninguna otra medida de carácter no legislativo para solucionar los problemas detectados por medio de la evaluación de la Directiva.
- Opción 1: no se producirían cambios a nivel legislativo. En su lugar, la Comisión publicaría recomendaciones y directrices (por ejemplo, sobre la identificación de operadores de servicios esenciales, los requisitos de seguridad, los procedimientos de notificación de incidentes y la supervisión), previa consulta con el Grupo de Cooperación, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y, en su caso, la red de equipos de respuesta a incidentes de seguridad informática (CSIRT).
- Opción 2: esta opción conlleva la realización de modificaciones focalizadas en la Directiva SRI, en particular, la ampliación del ámbito de aplicación y varias modificaciones adicionales con el objetivo de garantizar determinadas soluciones inmediatas a los problemas detectados, al aportar mayor claridad y armonización (p. ej., disposiciones para armonizar los umbrales de identificación). No obstante, la Directiva SRI conservaría los principales componentes, el enfoque y el fundamento.
- Opción 3: este escenario implica la realización de cambios sistémicos y estructurales en la Directiva SRI (a través de una nueva directiva) contemplando un cambio de enfoque más profundo destinado a abarcar un segmento más amplio de las economías de toda la Unión, aunque con una supervisión más centrada en los operadores clave y de grandes dimensiones. Asimismo, racionalizaría las obligaciones impuestas a las empresas y garantizaría un nivel más elevado de armonización de dichas obligaciones, crearía una configuración más efectiva para los aspectos operativos, y establecería unos cimientos claros para reforzar las responsabilidades compartidas y la rendición de cuentas de las diversas partes interesadas respecto a las medidas de ciberseguridad.

[7] **[Añádanse los enlaces al documento final y al resumen]**.

La evaluación de impacto determina que la opción preferida es la tercera, es decir, introducir cambios sistémicos y estructurales en el marco de la SRI. En términos de eficacia, la opción preferida delimitaría claramente el ámbito de aplicación de la Directiva SRI, ampliado para incluir una fracción más representativa de las economías y sociedades de la UE, y la racionalización de los requisitos, junto con un marco de supervisión y ejecución más preciso, aspiraría a incrementar el nivel de cumplimiento. También comprende medidas destinadas a mejorar los enfoques aplicados por los Estados miembros para el desarrollo de políticas y modificar su paradigma, mediante la promoción de nuevos marcos para la gestión de los riesgos derivados de las relaciones con los proveedores y una divulgación coordinada de las vulnerabilidades. Al mismo tiempo, la opción preferida establece unos cimientos claros para las responsabilidades compartidas y la rendición de cuentas y prevé mecanismos destinados a fomentar una confianza mayor entre los Estados miembros, así como entre las autoridades y la industria, incentivar el intercambio de información y garantizar un enfoque más operativo, como, por ejemplo, los mecanismos de asistencia mutua y de revisión interpares. Esta opción también contemplaría un marco de la UE para la gestión de crisis, apoyado en el marco operativo de la UE puesto en marcha recientemente, y aseguraría una implicación mayor de la ENISA, dentro de su mandato vigente, para tener una visión exacta de la situación de la Unión en materia de ciberseguridad.

Por lo que respecta a la eficiencia, a pesar de que la opción preferida conllevaría costes de conformidad y de ejecución adicionales para las empresas y los Estados miembros, también produciría compensaciones y sinergias eficientes, además de ser la opción que tiene un mejor potencial para garantizar un nivel reforzado y coherente de ciberresiliencia de las entidades clave de toda la Unión que, en última instancia, se traduciría en un ahorro de costes tanto para las empresas como para la sociedad. Esta opción generaría determinadas cargas administrativas y costes de conformidad adicionales para las autoridades de los Estados miembros. No obstante, en conjunto, a medio y largo plazo también aportaría beneficios significativos gracias a la mayor cooperación entre los Estados miembros, también a nivel operativo, e incentivaría, a través de la asistencia mutua, los mecanismos de revisión interpares y la mejora del panorama general de empresas clave y la interacción con estas, un incremento global de las capacidades de ciberseguridad a escala nacional y regional. Asimismo, la opción preferida garantizaría en gran medida la coherencia con otra legislación u otras iniciativas o medidas políticas, incluidas *lex specialis* sectoriales.

Resolver la persistente insuficiencia de la preparación en materia de ciberseguridad a escala de Estados miembros y de empresas y otras organizaciones podría traducirse en mejoras en términos de eficiencia y en la reducción de los costes adicionales derivados de los incidentes de ciberseguridad.

- Para las entidades esenciales e importantes, con el incremento del nivel de preparación en el ámbito de la ciberseguridad podrían mitigarse las posibles pérdidas de ingresos causadas por perturbaciones —también por el espionaje industrial— y reducirse las grandes cuantías destinadas a una reducción de amenazas *ad hoc*. Es probable que todos estos beneficios superen los costes de inversión necesarios. Reducir la fragmentación del mercado interior también mejoraría las condiciones de competencia equitativas entre los operadores.
- Para los Estados miembros, podría reducir en mayor medida el riesgo de incrementos en el gasto presupuestario para la reducción de amenazas *ad hoc* y costes adicionales en caso de emergencias relacionadas con incidentes de ciberseguridad.
- Para los ciudadanos, se espera que hacer frente a los incidentes de ciberseguridad se traduzca en una reducción de la pérdida de ingresos por perturbaciones económicas.

El aumento de los niveles de ciberseguridad en todos los Estados miembros y de la capacidad de las empresas y autoridades para responder con rapidez a un incidente y reducir su impacto muy probablemente se traduzca en un incremento de la confianza general de los ciudadanos en la economía digital, lo que podría repercutir positivamente en el crecimiento y la inversión.

Es probable que al aumentar el nivel global de ciberseguridad se produzca un incremento de la seguridad global y se logre el buen funcionamiento ininterrumpido de los servicios esenciales, fundamentales para la sociedad. Asimismo, la iniciativa puede generar otros efectos sociales, como una reducción de los niveles de ciberdelincuencia y terrorismo, y una mayor protección civil. Al incrementar el grado de preparación cibernética de las empresas y otras organizaciones es posible que se eviten posibles perjuicios financieros resultantes de ciberataques, evitando así la necesidad de despedir empleados.

Por otra parte, con un nivel global mayor de ciberseguridad se podrían prevenir riesgos/daños medioambientales en caso de que se produjesen ataques en servicios esenciales. Esta afirmación podría aplicarse en particular a los sectores de la energía, el suministro y la distribución de agua o el transporte. Mediante el refuerzo de las capacidades de ciberseguridad, la iniciativa podría potenciar el uso de infraestructuras y servicios de TIC de última generación, que también son más sostenibles desde el punto de vista medioambiental, y la sustitución de infraestructuras legadas ineficientes y menos seguras. Se espera que contribuya también a reducir el número de ciberincidentes costosos, liberando recursos para inversiones sostenibles.

- **Adecuación y simplificación de la normativa**

La propuesta prevé una exclusión general de las microentidades y las pequeñas entidades del ámbito de aplicación de la Directiva SRI y un régimen de supervisión *a posteriori* menos riguroso aplicado a un gran número de las nuevas entidades incluidas en el ámbito de aplicación revisado (las denominadas entidades importantes). El objetivo de estas medidas es minimizar y equilibrar la carga que soportan las empresas y las administraciones públicas. Por otra parte, la propuesta sustituye el complejo sistema de identificación de los operadores de servicios esenciales por una obligación de aplicación general e introduce un nivel más elevado de armonización de las obligaciones de seguridad y notificación que reduciría la carga asociada al cumplimiento, especialmente para las entidades que prestan servicios transfronterizos.

La propuesta minimiza los costes de conformidad para las pymes, ya que las entidades están obligadas a adoptar únicamente las medidas necesarias para garantizar un nivel de seguridad de las redes y sistemas de información adecuado al riesgo planteado.

- **Derechos fundamentales**

La UE se ha comprometido a garantizar unos niveles elevados de protección de los derechos fundamentales. Todos los mecanismos de intercambio voluntario de información entre entidades que la presente Directiva promueve se desarrollarían en entornos de confianza respetando plenamente las normas de protección de datos de la Unión, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[8].

[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).

4. REPERCUSIONES PRESUPUESTARIAS

Véase la ficha financiera.

5. OTROS ELEMENTOS

- **Planes de ejecución y disposiciones en materia de seguimiento, evaluación y notificación**

La propuesta incluye un plan general de seguimiento y evaluación del impacto en los objetivos específicos, en virtud del cual la Comisión debe efectuar una revisión al menos [cincuenta y cuatro meses] después de la fecha de entrada en vigor e informar de sus principales conclusiones al Parlamento Europeo y al Consejo.

La revisión debe llevarse a cabo con arreglo a las directrices para la mejora de la legislación de la Comisión.

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

La propuesta se articula en torno a varios ámbitos de actuación principales interrelacionados y cuyo objetivo es incrementar el nivel de ciberseguridad en la Unión.

Objeto y ámbito de aplicación (artículos 1 y 2)

En particular, la Directiva: a) establece obligaciones por las cuales los Estados miembros deben adoptar una estrategia nacional de ciberseguridad y designar autoridades nacionales competentes, puntos de contacto únicos y CSIRT; b) prevé que los Estados miembros establezcan obligaciones de gestión de riesgos de ciberseguridad y notificación para las entidades cuyo tipo se enmarca en el de las entidades esenciales del anexo I y en el de las entidades importantes del anexo II; c) contempla que los Estados miembros establezcan obligaciones relativas al intercambio de información sobre ciberseguridad.

Se aplica a determinadas entidades esenciales públicas o privadas que operan en los sectores recogidos en el anexo I (energía, transportes, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, Administración pública y sector espacial) y determinadas entidades importantes que operan en los sectores enumerados en el anexo II (servicios postales y de mensajería, gestión de residuos, fabricación, producción y distribución de sustancias y mezclas químicas, producción, transformación y distribución de alimentos, fabricación y proveedores de servicios digitales). Las microempresas y las pequeñas empresas en el sentido de la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, están excluidas del ámbito de aplicación de la Directiva, a excepción de los proveedores de redes de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, los prestadores de servicios de confianza, los registros de nombres de dominio de primer nivel y la Administración pública, así como otras entidades particulares, como por ejemplo los proveedores únicos de un servicio en un Estado miembro.

Marcos nacionales de ciberseguridad (artículos 5 a 11)

Los Estados miembros han de adoptar una estrategia nacional de ciberseguridad que establezca los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad.

Asimismo, la Directiva establece un marco para la divulgación coordinada de las vulnerabilidades y obliga a los Estados miembros a designar CSIRT que ejerzan de intermediarios de confianza y faciliten la interacción entre las entidades notificantes y los fabricantes o proveedores de productos y servicios de TIC. La ENISA debe desarrollar y mantener un Registro Europeo de Vulnerabilidades en el que se introduzcan las vulnerabilidades detectadas.

Los Estados miembros deben instaurar marcos nacionales de gestión de crisis de ciberseguridad, entre otros, mediante la designación de las autoridades nacionales competentes encargadas de gestionar los incidentes y las crisis de ciberseguridad a gran escala.

Asimismo, deben designar una o varias autoridades nacionales competentes en el ámbito de la ciberseguridad que se ocupen de las tareas de supervisión previstas en la presente Directiva y un punto nacional de contacto único para la ciberseguridad que ejerza de enlace para garantizar la cooperación transfronteriza de las autoridades de los Estados miembros. Además, los Estados miembros deben designar CSIRT.

Cooperación (artículos 12 a 16)

La Directiva establece un Grupo de Cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y la seguridad. Por otra parte, establece una red de CSIRT para contribuir al desarrollo de la confianza y la seguridad entre los Estados miembros y promover una cooperación operativa ágil y efectiva.

Se crea una red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) para apoyar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala y para garantizar el intercambio de información regular entre los Estados miembros y las instituciones de la UE.

La ENISA debe publicar, en cooperación con la Comisión, un informe bienal sobre la situación de la ciberseguridad en la Unión.

La Comisión debe establecer un sistema de revisión interpares que permita una revisión interpares regular de la eficacia de las políticas de ciberseguridad de los Estados miembros.

Obligaciones de gestión de riesgos de ciberseguridad y notificación (artículos 17 a 23)

La Directiva requiere que los Estados miembros prevean que los órganos de dirección de todas las entidades incluidas en el ámbito de aplicación aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por las respectivas entidades y reciban formación específica relacionada con la ciberseguridad.

Los Estados miembros deben velar por que las entidades incluidas en el ámbito de aplicación adopten medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad existentes para la seguridad de las redes y los sistemas de información. Asimismo, deben velar por que las entidades notifiquen a las autoridades nacionales competentes o a los CSIRT cualquier incidente de ciberseguridad que tenga efectos significativos en la prestación de sus servicios.

Los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel han de recopilar y mantener datos precisos y completos sobre el registro de nombres de dominio. Además, estas entidades deben facilitar un acceso eficiente a los datos de registro de dominios a los solicitantes de acceso legítimos.

Jurisdicción y registro (artículos 24 y 25)

Como norma general, se considera que las entidades esenciales e importantes están sometidas a la jurisdicción del Estado miembro en el que prestan sus servicios. No obstante, determinados tipos de entidades (los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de redes de distribución de contenidos, así como los proveedores de servicios digitales) se consideran sometidos a la jurisdicción del Estado miembro en el que se encuentra su establecimiento principal en la Unión. La finalidad de esto es garantizar que dichas entidades no se enfrenten a multitud de requisitos legales diferentes, ya que en su caso concreto prestan servicios transfronterizos con mucha frecuencia. La ENISA tiene la obligación de crear y mantener un registro de este último tipo de entidades.

Intercambio de información (artículos 26 y 27)

Los Estados miembros deben prever normas que permitan a las entidades participar en el intercambio de información sobre ciberseguridad en el marco de mecanismos específicos destinados al intercambio de información de esta índole, de conformidad con el artículo 101 del TFUE. Por otro lado, los Estados miembros deben permitir que las entidades excluidas del ámbito de aplicación de esta Directiva notifiquen voluntariamente ciberamenazas, cuasiincidentes e incidentes significativos.

Supervisión y ejecución (artículos 28 a 34)

Las autoridades competentes están obligadas a supervisar las entidades incluidas en el ámbito de aplicación de la Directiva y, en particular, a velar por que cumplan los requisitos de seguridad y notificación de incidentes. En la Directiva se distingue entre un régimen de supervisión *a priori* para las entidades esenciales y un régimen de supervisión *a posteriori* para las entidades importantes. Este último requiere que las autoridades competentes emprendan medidas cuando dispongan de pruebas o indicios de que una entidad importante no cumple los requisitos de seguridad y notificación de incidentes.

Asimismo, la Directiva obliga a los Estados miembros a imponer multas administrativas a las entidades esenciales e importantes y define determinadas multas máximas.

Los Estados miembros deben cooperar entre sí y prestarse asistencia mutua, siempre que sea necesario, cuando las entidades presten servicios en más de un Estado miembro o cuando el establecimiento principal de una entidad o su representante se encuentren en un Estado miembro determinado, pero sus redes y sistemas de información estén ubicados en otros Estados miembros.

2020/0359 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

(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[9],

Visto el dictamen del Comité de las Regiones[10],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[11] era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para las redes y los sistemas de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes de ciberseguridad, contribuyendo así al funcionamiento eficaz de la economía y la sociedad de la Unión.

(2) Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han realizado considerables progresos en el incremento del nivel de resiliencia en materia de ciberseguridad de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y reglamentario relativo a la ciberseguridad en la Unión, preparando el camino para un cambio significativo de mentalidad. Con ella se ha logrado la realización de marcos nacionales mediante la definición de las estrategias nacionales de ciberseguridad, el establecimiento de las capacidades nacionales y la aplicación de medidas reglamentarias que abarcan a los actores y las infraestructuras esenciales identificados por cada Estado miembro. Asimismo, ha propiciado la cooperación a nivel de la Unión mediante el establecimiento del Grupo de Cooperación[12] y de una red de equipos de respuesta a

[9] DO C […] de […], p. […].

[10] DO C […] de […], p. […].

[11] 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).

[12] Artículo 11 de la Directiva (UE) 2016/1148.

incidentes de seguridad informática («Red de CSIRT»)[13]. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes que impiden un abordaje eficaz de los retos contemporáneos y emergentes en el ámbito de la ciberseguridad.

(3) Las redes y los sistemas de información se han convertido en un aspecto indispensable del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad, también en los intercambios transfronterizos. Esta evolución ha causado una expansión del panorama de amenazas de ciberseguridad, con la consiguiente aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes de ciberseguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Como consecuencia de ello, los incidentes cibernéticos pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, menoscabar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión. Por consiguiente, la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca para que el mercado interior funcione correctamente.

(4) La base jurídica de la Directiva (UE) 1148/2016 era el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), cuyo objetivo es el establecimiento y el funcionamiento del mercado interior mediante el refuerzo de las medidas destinadas a la aproximación de las normas nacionales. Los requisitos de ciberseguridad que se imponen a las entidades que prestan servicios o actividades pertinentes desde el punto de vista económico varían considerablemente en función del Estado miembro por lo que respecta al tipo de requisito, su nivel de detalle y el método de supervisión. Estas disparidades conllevan costes adicionales y generan dificultades para las empresas que ofrecen productos o servicios transfronterizos. Los requisitos impuestos por un Estado miembro que difieren de los aplicados por otro Estado miembro, o incluso los contradicen, pueden afectar sustancialmente a las mencionadas actividades transfronterizas. Además, es probable que una concepción o una aplicación subóptimas de las normas de ciberseguridad en un Estado miembro tenga repercusiones para el nivel de ciberseguridad de otros Estados miembros, especialmente habida cuenta de la intensidad de los intercambios transfronterizos. La revisión de la Directiva (UE) 2016/1148 ha demostrado la existencia de grandes diferencias en su aplicación por parte de los Estados miembros, en particular por lo que respecta a su ámbito de aplicación, cuya delimitación se dejó en gran medida a discreción de los Estados miembros. Asimismo, la Directiva (UE) 2016/1148 confería a los Estados miembros una discrecionalidad muy amplia en lo tocante a la aplicación de las obligaciones de seguridad y notificación de incidentes en ella establecidas. En consecuencia, dichas obligaciones se aplicaron de maneras considerablemente diferentes a escala nacional. Se observaron diferencias similares en la aplicación de las disposiciones relativas a la supervisión y la ejecución de la Directiva.

(5) Todas esas diferencias conllevan una fragmentación del mercado interior y pueden tener un efecto perjudicial para su funcionamiento, afectando, en particular, a la prestación transfronteriza de servicios y al nivel de resiliencia en el ámbito de la ciberseguridad debido a la aplicación de normas diferentes. El objetivo de la presente

[13] Artículo 12 de la Directiva (UE) 2016/1148.

Directiva es eliminar estas divergencias tan pronunciadas entre los Estados miembros, concretamente mediante el establecimiento de las normas mínimas relativas al funcionamiento de un marco reglamentario coordinado, la fijación de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera efectiva, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la facilitación de vías de recurso y sanciones eficaces que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones. Por consiguiente, procede derogar la Directiva (UE) 2016/1148 y sustituirla por la presente Directiva.

(6) La presente Directiva no afecta a la capacidad de los Estados miembros de adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de su seguridad, preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales, con arreglo al Derecho de la Unión. De conformidad con el artículo 346 del TFUE, ningún Estado miembro está obligado a facilitar información cuya divulgación sería contraria a los intereses esenciales de su seguridad pública. En este contexto, son pertinentes las normas nacionales y de la Unión en materia de protección de la información clasificada, los acuerdos sobre confidencialidad y los acuerdos de confidencialidad informales como el Protocolo TLP para el intercambio de información[14].

(7) Con la derogación de la Directiva (UE) 2016/1148, es preciso hacer extensivo el ámbito de aplicación por sectores a una parte mayor de la economía, habida cuenta de las consideraciones expuestas en los considerandos 4 a 6. En consecuencia, los sectores amparados por la Directiva (UE) 2016/1148 deben ampliarse para ofrecer una cobertura global de los sectores y servicios de vital importancia para las actividades sociales y económicas fundamentales dentro del mercado interior. Las normas no deben ser diferentes según las entidades sean operadores de servicios esenciales o proveedores de servicios digitales. Dicha diferenciación ha quedado obsoleta, ya que no refleja la importancia real de los sectores o servicios para las actividades sociales y económicas en el mercado interior.

(8) Con arreglo a lo dispuesto en la Directiva (UE) 2016/1148, los Estados miembros eran responsables de determinar qué entidades cumplían los criterios para que se considerasen operadores de servicios esenciales («proceso de identificación»). A fin de eliminar las profundas divergencias entre los Estados miembros en ese sentido y garantizar seguridad jurídica para todas las entidades pertinentes respecto a los requisitos de gestión del riesgo y las obligaciones de notificación, debe establecerse un criterio uniforme que determine las entidades que están incluidas en el ámbito de aplicación de la presente Directiva. Dicho criterio debe consistir en la aplicación de la norma sobre el tamaño máximo, por la que todas las empresas medianas y grandes, conforme a la definición recogida en la Recomendación 2003/361/CE de la Comisión[15], que operen en los sectores o presten el tipo de servicios amparados por la presente Directiva queden incluidos en su ámbito de aplicación. Los Estados

[14] El Protocolo TLP para el intercambio de información es un medio que permite a todo aquel que comparta información comunicar a los destinatarios las posibles limitaciones a la divulgación ulterior de dicha información. Se utiliza en prácticamente todas las comunidades de CSIRT y en algunos Centros de puesta en común y análisis de la información.

[15] 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).

miembros no deben estar obligados a establecer una lista de las entidades que se ajustan a este criterio asociado al tamaño de aplicación general.

(9) No obstante, la presente Directiva también debe ser aplicable a las microentidades o pequeñas entidades que cumplan determinados criterios que indiquen que desempeñan un papel clave para las economías o las sociedades de los Estados miembros, o en el caso de sectores o tipos de servicios concretos. Los Estados miembros deben encargarse de elaborar la lista de tales entidades y presentarla a la Comisión.

(10) La Comisión, en cooperación con el Grupo de Cooperación, puede publicar directrices sobre la aplicación de los criterios aplicables a las microempresas y pequeñas empresas.

(11) En función del sector en el que operen o el tipo de servicio que presten, las entidades incluidas en el ámbito de aplicación de la presente Directiva se clasificarán en dos categorías: esenciales e importantes. Dicha clasificación debe tener en cuenta el nivel de criticidad del sector o del tipo de servicio, así como el grado de dependencia de otros sectores o tipos de servicios. Las entidades esenciales e importantes han de estar sujetas a los mismos requisitos de gestión del riesgo y a las mismas obligaciones de notificación. Los regímenes de supervisión y de sanciones deben ser diferentes para las dos categorías de entidades, a fin de garantizar un equilibrio justo entre los requisitos y las obligaciones, por un lado, y la carga administrativa derivada de la supervisión del cumplimiento, por el otro.

(12) La legislación y los instrumentos sectoriales pueden contribuir a garantizar unos niveles elevados de ciberseguridad, al tiempo que se tienen plenamente en cuenta las especificidades y complejidades de dichos sectores. Cuando un acto jurídico de la Unión de carácter sectorial exija a las entidades esenciales o importantes adoptar medidas para la gestión de riesgos de ciberseguridad o notificar los incidentes o las ciberamenazas significativas con un efecto al menos equivalente al de las obligaciones establecidas en la presente Directiva, deberán aplicarse dichas disposiciones sectoriales, incluidas las relativas a la supervisión y la ejecución La Comisión puede publicar directrices en relación con la aplicación de la *lex specialis*. La presente Directiva no impide que se adopten actos sectoriales de la Unión adicionales que aborden las medidas para la gestión de los riesgos de ciberseguridad y las notificaciones de incidentes. Asimismo, la Directiva debe entenderse sin perjuicio de las competencias de ejecución existentes que se han conferido a la Comisión en varios sectores, como, por ejemplo, el del transporte y la energía.

(13) El Reglamento XXXX/XXXX del Parlamento Europeo y del Consejo[16] debe considerarse un acto jurídico de la Unión de carácter sectorial en relación con la presente Directiva por lo que respecta a las entidades del sector financiero. En lugar de las disposiciones contempladas en la presente Directiva, deben aplicarse las disposiciones del Reglamento XXXX/XXXX relativas a las medidas de gestión de los riesgos de las tecnologías de la información y de las comunicaciones (TIC), a la gestión de los incidentes asociados a las TIC, en particular la notificación de los mismos, así como a las pruebas de la resiliencia operativa digital, los mecanismos de intercambio de información y el riesgo de terceros relacionado con las TIC. En consecuencia, los Estados miembros no deben aplicar las disposiciones de la presente Directiva relativas a las obligaciones de gestión de los riesgos de ciberseguridad y de notificación, intercambio de información, y supervisión y ejecución a ninguna entidad

[16] *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

financiera cubierta por el Reglamento XXXX/XXXX. Al mismo tiempo, conviene mantener una estrecha relación y el intercambio de información con el sector financiero al amparo de la presente Directiva. Para ello, el Reglamento XXXX/XXXX permite que todos los supervisores financieros, las Autoridades Europeas de Supervisión (AES) para el sector financiero y las autoridades nacionales competentes en virtud del Reglamento XXXX/XXXX participen en los debates estratégicos y en los trabajos técnicos del Grupo de Cooperación e intercambien información y cooperen con los puntos de contacto únicos designados con arreglo a la presente Directiva y con los CSIRT nacionales. Las autoridades competentes conforme al Reglamento XXXX/XXXX deben transmitir los detalles de los incidentes graves relacionados con las TIC también a los puntos de contacto únicos designados en virtud de la presente Directiva. Además, los Estados miembros deben seguir incluyendo al sector financiero en sus estrategias de ciberseguridad y los CSIRT nacionales pueden ocuparse del sector financiero en sus actividades.

(14) En vista de los vínculos que existen entre la ciberseguridad y la seguridad física de las entidades, debe garantizarse un enfoque coherente entre la Directiva (UE) XXX/XXX del Parlamento Europeo y del Consejo[17] y la presente Directiva. Para ello, los Estados miembros han de velar por que las entidades críticas, y las entidades equivalentes conforme a lo dispuesto en la Directiva (UE) XXX/XXX, se consideren entidades esenciales a los efectos de la presente Directiva. Asimismo, los Estados miembros deben asegurarse de que sus estrategias de ciberseguridad prevean un marco político para una coordinación reforzada entre las autoridades competentes con arreglo a la presente Directiva y las competentes en virtud de la Directiva (UE) XXX/XXX en el contexto del intercambio de información sobre incidentes y ciberamenazas y el ejercicio de las tareas de supervisión. Las autoridades competentes al amparo de ambas Directivas deben cooperar e intercambiar información, en particular en relación con la identificación de las entidades críticas, las ciberamenazas, los riesgos de ciberseguridad y los incidentes que afecten a las entidades críticas, así como con las medidas de ciberseguridad adoptadas por estas entidades. A instancias de las autoridades competentes en virtud de la Directiva (UE) XXX/XXX, las autoridades competentes a los efectos de la presente Directiva deben poder ejercer sus facultades de supervisión y ejecución respecto a una entidad esencial identificada como crítica. Ambas autoridades deben cooperar e intercambiar información para tal fin.

(15) El mantenimiento y la conservación de un sistema de nombres de dominio (DNS) fiable, resiliente y seguro son factores clave para garantizar la integridad de internet y resultan fundamentales para que funcione con estabilidad y de manera ininterrumpida, de lo que depende la economía digital y la sociedad. Por consiguiente, la presente Directiva debe aplicarse a todos los proveedores de servicios de DNS a lo largo de la cadena de resolución de DNS, incluidos los operadores de servidores raíz, servidores de nombres de dominio de primer nivel, servidores de nombres autoritativos para nombres de dominio y solucionadores recursivos.

(16) Los servicios de computación en nube deben abarcar los servicios que permiten un acceso remoto bajo demanda y amplio a un conjunto modulable y elástico de recursos informáticos distribuidos que se pueden compartir. Esos recursos informáticos incluyen recursos tales como las redes, los servidores u otras infraestructuras, sistemas operativos, *software*, almacenamiento, aplicaciones y servicios. Los modelos de

[17] *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

despliegue de la computación en nube deben abarcar nubes privadas, comunitarias, públicas e híbridas. Los referidos modelos de servicio y despliegue tienen el mismo significado que los términos de los modelos de servicio y despliegue definidos en la norma ISO/IEC 17788:2014. La capacidad del usuario de la computación en nube de autoabastecerse unilateralmente de capacidades de computación, como, por ejemplo, tiempo de servidor o almacenamiento en red, sin ninguna interacción humana por parte del proveedor de servicios de computación en nube podría describirse como administración bajo demanda. La expresión «acceso remoto amplio» se utiliza para describir que las capacidades en la nube se suministran en toda la red y se accede a ellas a través de mecanismos que promueven el uso de plataformas de cliente ligero o pesado heterogéneas (incluidos teléfonos móviles, tabletas, ordenadores portátiles o estaciones de trabajo). El término «modulable» se refiere a los recursos informáticos que el proveedor de servicios en nube puede asignar de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término «elástico» se usa para describir los recursos de los que se abastece y que se ponen a la venta según la demanda, de modo que se puedan aumentar o reducir con rapidez los recursos disponibles en función de la carga de trabajo. La expresión «que se pueden compartir» se usa para describir recursos informáticos que se proporcionan a múltiples usuarios que comparten un acceso común al servicio pero el tratamiento se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico. El término «distribuido» se emplea para describir los recursos informáticos que se encuentran ubicados en distintos ordenadores o dispositivos conectados en red y que se comunican y coordinan entre sí intercambiando mensajes.

(17) Habida cuenta de la aparición de tecnologías innovadoras y nuevos modelos de negocio, se espera que surjan en el mercado nuevos modelos de despliegue y servicio de computación en nube en respuesta a la evolución de las necesidades de los clientes. En ese contexto, los servicios de computación en nube pueden prestarse de una forma muy distribuida, más cerca si cabe del punto en que los datos se generan o recogen, abandonando así el modelo tradicional en favor de uno muy distribuido («computación en el borde»)

(18) Los servicios ofrecidos por los proveedores de servicios de centro de datos no siempre pueden prestarse en forma de servicio de computación en nube. En consecuencia, los centros de datos no siempre pueden formar parte de una infraestructura de computación en nube. A fin de gestionar todos los riesgos que se plantean para la seguridad de las redes y sistemas de información, la presente Directiva también debe englobar a los proveedores de estos servicios de centro de datos que no son servicios de computación en nube. A los efectos de la presente Directiva, la expresión «servicio de centro de datos» debe abarcar la prestación de un servicio que englobe las estructuras, o agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de tecnologías de la información y equipos de red que proporcionen servicios de almacenamiento, tratamiento y transporte de datos, junto con todas las instalaciones e infraestructuras destinadas a la distribución de energía y el control ambiental. La expresión «servicio de centro de datos» no se aplica a los centros de datos empresariales internos cuya propiedad y explotación para fines propios dependen de la entidad de que se trate.

(19) Los proveedores de servicios postales en el sentido de la Directiva 97/67/CE del Parlamento Europeo y del Consejo[18], así como los proveedores de servicios de envío urgente y mensajería, deben estar sujetos a la presente Directiva si se ocupan de al menos una de las fases de la cadena de distribución postal y en particular de la recogida, la clasificación o la distribución, incluida la recogida por el destinatario. Los servicios de transporte que no se lleven a cabo en combinación con alguna de estas etapas deben quedar excluidos del ámbito de los servicios postales.

(20) Estas crecientes interdependencias obedecen a una red cada vez más transfronteriza e interdependiente de prestaciones de servicios que utilizan infraestructuras clave de toda la Unión en los sectores de la energía, el transporte, la infraestructura digital, el agua potable y las aguas residuales, la sanidad, determinados aspectos de la Administración pública, así como el espacio por lo que respecta a la prestación de determinados servicios que dependen de infraestructuras terrestres cuya propiedad, gestión y explotación residen en los Estados miembros o en entidades privadas, dejando al margen, por tanto, las infraestructuras cuya propiedad, gestión u explotación dependen de la Unión o se efectúan en su nombre como parte de sus programas espaciales. Tales interdependencias implican que cualquier perturbación, incluso aquellas que inicialmente se circunscriben a una entidad o un sector, puede tener efectos en cascada más amplios que pueden dar lugar a impactos con un gran alcance y duración en la prestación de servicios en todo el mercado interior. La pandemia de COVID-19 ha puesto de relieve la vulnerabilidad de nuestras sociedades, cada vez más interdependientes, ante riesgos con probabilidad baja.

(21) Habida cuenta de las diferencias existentes entre las estructuras nacionales de gobernanza y con el fin de salvaguardar las disposiciones sectoriales vigentes o los organismos de supervisión y regulación de la Unión ya existentes, los Estados miembros deben poder designar a más de una autoridad nacional competente responsable de ejercer las tareas vinculadas a la seguridad de las redes y los sistemas de información de las entidades esenciales e importantes en virtud de la presente Directiva. Los Estados miembros deben poder asignar esta función a una autoridad existente.

(22) Con el fin de facilitar la cooperación y la comunicación transfronterizas entre las autoridades y de permitir una aplicación efectiva de la presente Directiva, es necesario que cada Estado miembro designe un punto de contacto único nacional que se encargue de coordinar las cuestiones relacionadas con la seguridad de las redes y sistemas de información y de la cooperación transfronteriza a escala de la Unión.

(23) Las autoridades competentes o los CSIRT deben recibir las notificaciones de los incidentes enviadas por las entidades de manera eficaz y eficiente. Debe encomendarse a los puntos de contacto único la transmisión de las notificaciones de incidentes a los puntos de contacto único de otros Estados miembros afectados. A escala de las autoridades de los Estados miembros, a fin de garantizar un único punto de entrada en cada Estado miembro, los puntos de contacto único también deben ser los destinatarios de la información pertinente sobre incidentes relativos a entidades del sector financiero enviada por las autoridades competentes en virtud del Reglamento XXXX/XXXX, que

[18] Directiva 97/67/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio (DO L 15 de 21.1.1998, p. 14).

deben poder transmitir, según proceda, a las correspondientes autoridades nacionales competentes o a los CSIRT con arreglo a la presente Directiva.

(24) Los Estados miembros deben disponer de capacidades técnicas y de organización adecuadas para poder adoptar medidas de prevención, detección, respuesta y reducción de los incidentes y riesgos que afecten a las redes y sistemas de información. Por tanto, los Estados miembros deben asegurarse de que disponen de CSIRT, también denominados equipos de respuesta a emergencias informáticas (CERT®, por sus siglas en inglés), que funcionen adecuadamente y cumplan los requisitos esenciales para así disponer de capacidades efectivas y compatibles que permitan hacer frente a incidentes y riesgos y garantizar una cooperación eficaz a escala de la Unión. Con vistas a reforzar la relación de confianza entre las entidades y los CSIRT, cuando un CSIRT forme parte de una autoridad competente, los Estados miembros deben considerar la posibilidad de establecer una separación funcional entre las tareas operativas desempeñadas por los CSIRT, en particular en relación con el intercambio de información y el apoyo prestado a las entidades, y las actividades de supervisión de las autoridades competentes.

(25) Por lo que respecta a los datos personales, los CSIRT deben poder ofrecer, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[19] una exploración proactiva de las redes y los sistemas de información utilizados para la prestación de sus servicios en nombre de una entidad amparada por la presente Directiva y a petición de ella. Los Estados miembros deben tratar de garantizar el mismo nivel de capacidades técnicas para todos los CSIRT sectoriales. Los Estados miembros pueden solicitar la asistencia de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) a la hora de crear CSIRT nacionales.

(26) Dada la importancia de la cooperación internacional en materia de ciberseguridad, los CSIRT deben tener la posibilidad de participar en redes internacionales de cooperación además de la red de CSIRT establecida en virtud de la presente Directiva.

(27) De conformidad con al anexo de la Recomendación (UE) 2017/1548 de la Comisión, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (Plan director)[20], por incidente a gran escala debe entenderse un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros. Dependiendo de su causa e impacto, los incidentes a gran escala pueden intensificarse y convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior. Habida cuenta de la amplitud del alcance y, en la mayoría de casos, de la naturaleza transfronteriza de tales incidentes, los Estados miembros y las instituciones, los órganos y los organismos de la Unión pertinentes deben cooperar a nivel técnico, operativo y político para coordinar convenientemente la respuesta en toda la Unión.

(28) Puesto que la explotación de las vulnerabilidades de las redes y sistemas de información puede causar perturbaciones y daños considerables, la determinación y subsanación rápidas de dichas vulnerabilidades son factores importantes para reducir

---

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

20 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).

los riesgos de ciberseguridad. En consecuencia, las entidades que desarrollen sistemas a tales efectos deben establecer procedimientos apropiados para manejar las vulnerabilidades cuando se detecten. Teniendo en cuenta que las vulnerabilidades suelen ser detectadas y notificadas (reveladas) por terceros (entidades notificantes), los fabricantes o proveedores de productos o servicios de TIC también deben implantar los procedimientos necesarios para recibir información sobre las vulnerabilidades de terceros. En este sentido, las normas internacionales ISO/IEC 30111 e ISO/IEC 29417 ofrecen orientación sobre el manejo de las vulnerabilidades y la divulgación de las vulnerabilidades respectivamente. Por lo que respecta a la divulgación de las vulnerabilidades, la coordinación entre las entidades notificantes y los fabricantes o proveedores de productos o servicios de TIC reviste una gran importancia. La divulgación coordinada de las vulnerabilidades especifica un proceso estructurado a través del cual las vulnerabilidades se notifican a las organizaciones de tal manera que estas puedan diagnosticar y subsanar las vulnerabilidades antes de revelar información detallada sobre ellas a terceros o al público. Asimismo, la divulgación coordinada de las vulnerabilidades debe comprender la coordinación entre la entidad notificante y la organización en lo tocante al momento de la subsanación y la publicación de las vulnerabilidades.

(29) Por consiguiente, los Estados miembros deben adoptar medidas para facilitar la divulgación coordinada de las vulnerabilidades mediante el establecimiento de la correspondiente política nacional. A este respecto, los Estados miembros deben designar un CSIRT que asuma el papel de «coordinador» y ejerza de intermediario entre las entidades notificantes y los fabricantes o proveedores de productos o servicios de TIC cuando sea necesario. Las tareas del CSIRT coordinador deben consistir, en particular, en identificar a las entidades afectadas y contactar con ellas, prestar apoyo a las entidades notificantes, negociar los plazos de divulgación y manejar las vulnerabilidades que afectan a múltiples organizaciones (divulgación de las vulnerabilidades con múltiples interesados). Cuando las vulnerabilidades afecten a múltiples fabricantes o proveedores de productos o servicios de TIC establecidos en más de un Estado miembro, los CSIRT designados de cada Estado miembro afectado deben cooperar en el marco de la red de CSIRT.

(30) El acceso a información correcta y oportuna sobre las vulnerabilidades que afectan a productos y servicios de TIC contribuye a reforzar la gestión de los riesgos de ciberseguridad. En este sentido, las fuentes de información sobre las vulnerabilidades disponibles para el público suponen una herramienta importante para las entidades y sus usuarios, pero también para las autoridades nacionales competentes y los CSIRT. Por este motivo, la ENISA debe crear un registro de vulnerabilidades en el que las entidades esenciales e importantes y sus proveedores, así como las entidades que no estén incluidas en el ámbito de aplicación de la presente Directiva, puedan, de manera voluntaria, revelar las vulnerabilidades y facilitar información sobre las mismas que permita a los usuarios adoptar las medidas de mitigación apropiadas.

(31) Aunque efectivamente existen registros o bases de datos de vulnerabilidades similares, su alojamiento y mantenimiento dependen de entidades que no están establecidas en la Unión. Con un Registro Europeo de Vulnerabilidades mantenido por la ENISA se conseguiría mejorar la transparencia del proceso de publicación antes de que la vulnerabilidad se revele oficialmente y la resiliencia en caso de perturbaciones o interrupciones de la prestación de servicios similares. A fin de evitar la duplicación de esfuerzos y lograr la complementariedad en la medida de lo posible, la ENISA debe

estudiar la posibilidad de celebrar acuerdos de cooperación estructurada con registros similares en jurisdicciones de terceros países.

(32) El Grupo de Cooperación debe elaborar cada dos años un programa de trabajo que comprenda las acciones que llevará a cabo para poner en práctica sus objetivos y cometidos. El calendario del primer programa adoptado en virtud de la presente Directiva debe adecuarse al del último programa adoptado con arreglo a la Directiva (UE) 2016/1148 para evitar posibles perturbaciones en el trabajo del Grupo.

(33) A la hora de elaborar documentos de orientación, de manera sistemática el Grupo de Cooperación debe identificar las soluciones y experiencias nacionales, evaluar el impacto de los resultados concretos del Grupo de Cooperación en los enfoques nacionales, debatir los desafíos en materia de aplicación y formular recomendaciones específicas que deben incorporarse mediante la mejora de la aplicación de las normas vigentes.

(34) El Grupo de Cooperación debe seguir siendo un foro flexible y capaz de responder a prioridades y desafíos políticos nuevos y cambiantes, teniendo en cuenta a la vez la disponibilidad de los recursos. Debe organizar reuniones conjuntas periódicas con las partes interesadas privadas pertinentes de toda la Unión para debatir las actividades realizadas por el Grupo y recabar apreciaciones sobre los desafíos políticos emergentes. Con vistas a reforzar la cooperación a escala de la Unión, el Grupo debe considerar la posibilidad de invitar a que participen en sus actividades a los órganos y las agencias de la Unión implicados en la política de ciberseguridad, como por ejemplo el Centro Europeo de Ciberdelincuencia (EC3), la Agencia de la Unión Europea para la Seguridad Aérea (AESA) y la Agencia de la Unión Europea para el Programa Espacial (EUSPA).

(35) Las autoridades competentes y los CSIRT deben estar capacitados para participar en programas de intercambio para funcionarios de otros Estados miembros para mejorar la cooperación. Las autoridades competentes deben adoptar las medidas necesarias para que los funcionarios de otros Estados miembros puedan desempeñar un papel eficaz en las actividades de la autoridad competente de acogida.

(36) La Unión debe celebrar, cuando corresponda y de conformidad con el artículo 218 del TFUE, acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades del Grupo de Cooperación y la red de CSIRT. Dichos acuerdos deben velar por una protección de datos adecuada.

(37) Los Estados miembros deben contribuir al establecimiento del Marco de respuesta a las crisis de ciberseguridad de la UE recogido en la Recomendación (UE) 2017/1584 a través de las redes de cooperación existentes, en particular la red de organizaciones de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe), la red de CSIRT y el Grupo de Cooperación. La EU-CyCLONe y la red de CSIRT deben cooperar sobre la base de disposiciones de procedimiento que definan las modalidades de dicha cooperación. El reglamento interno de la EU-CyCLONe debe especificar asimismo las modalidades por las que debe regirse el funcionamiento de la red, incluidos, entre otros, las funciones, los modos de cooperación, las interacciones con otros actores pertinentes y los modelos para el intercambio de información, así como los medios de comunicación. De cara a la gestión de crisis a escala de la Unión, las partes pertinentes deben recurrir al Dispositivo de la UE de Respuesta Política Integrada a las Crisis (RPIC). La Comisión debe utilizar a tales efectos el proceso de coordinación de crisis intersectoriales de alto nivel ARGUS. Si la crisis tiene una importante dimensión de

política exterior o de política común de seguridad y defensa (PCSD), debe activarse el Mecanismo de Respuesta a las Crisis (CRM) del Servicio Europeo de Acción Exterior (SEAE).

(38) A los efectos de la presente Directiva, el término «riesgo» deben entenderse como las posibles pérdidas o perturbaciones causadas por un incidente de ciberseguridad y debe expresarse como una combinación de la magnitud de tales pérdidas o perturbaciones y la probabilidad de que se produzca dicho incidente.

(39) Asimismo, el término «cuasiincidente» debe entenderse como cualquier suceso que podría haber causado daños, pero cuya materialización completa se previno de manera satisfactoria.

(40) Entre las medidas de gestión del riesgo deben figurar aquellas cuya finalidad es determinar todo riesgo de incidentes, prevenir, detectar y gestionar incidentes y reducir sus repercusiones. La seguridad de las redes y los sistemas de información debe comprender la seguridad de los datos almacenados, transmitidos y tratados.

(41) Para evitar imponer una carga financiera y administrativa desproporcionada a las entidades esenciales e importantes, los requisitos de gestión de los riesgos de ciberseguridad han de ser proporcionados en relación con los riesgos que presentan la red y el sistema de información en cuestión, y tener en cuenta el estado de la técnica.

(42) Las entidades esenciales e importantes deben garantizar la seguridad de las redes y los sistemas de información que utilizan en sus actividades. Se trata fundamentalmente de redes y sistemas de información privados gestionados por el personal informático interno o cuya seguridad se ha encomendado a empresas externas. Los requisitos de gestión de riesgos de ciberseguridad y de notificación en virtud de la presente Directiva deben aplicarse a las entidades esenciales e importantes pertinentes, independientemente de si se encargan ellas mismas del mantenimiento de sus redes y sistemas de información o lo externalizan.

(43) Hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad y su relación con sus proveedores resulta especialmente importante, habida cuenta de la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y los agentes malintencionados han podido comprometer la seguridad de las redes y los sistemas de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Por ello, las entidades deben evaluar y tener en cuenta la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

(44) Entre los proveedores de servicios, los proveedores de servicios de seguridad administrada en ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría desempeñan un papel especialmente importante al prestar asistencia a las entidades en sus esfuerzos por detectar los incidentes y responder a ellos. No obstante, los propios proveedores de servicios de seguridad administrada también han sido objetivo de ciberataques y plantean un riesgo de ciberseguridad especial como consecuencia de su estrecha integración en los procesos de los operadores. En consecuencia, las entidades deben redoblar su diligencia a la hora de seleccionar un proveedor de servicios de seguridad administrada.

(45) Asimismo, las entidades deben abordar los riesgos de ciberseguridad derivados de sus interacciones y relaciones con otras partes interesadas dentro de un ecosistema más

amplio. Concretamente, las entidades han de adoptar las medidas oportunas para garantizar que su cooperación con las instituciones académicas y de investigación se desarrolle de acuerdo con sus políticas de ciberseguridad y siga buenas prácticas por lo que respecta a la seguridad del acceso y la divulgación de información en general y la protección de la propiedad intelectual en particular. De igual manera, dada la importancia y el valor de los datos para las actividades de las entidades, estas deben adoptar todas las medidas de ciberseguridad apropiadas cuando recurran a servicios de transformación de datos y análisis de datos de terceros.

(46) Para abordar en mayor profundidad los principales riesgos de la cadena de suministro y ayudar a las entidades que operan en los sectores incluidos en el ámbito de aplicación de la presente Directiva a gestionar adecuadamente los riesgos de ciberseguridad asociados a la cadena de suministro y los proveedores, el Grupo de Cooperación, con la participación de las autoridades nacionales pertinentes y en colaboración con la Comisión y la ENISA, debe llevar a cabo evaluaciones coordinadas sectoriales de los riesgos de la cadena de suministro, como ya se hizo en el caso de las redes 5G a raíz de la Recomendación (UE) 2019/534 sobre la ciberseguridad de las redes 5G[21], con el objetivo de identificar cuáles son los servicios, sistemas o productos de TIC críticos, las correspondientes amenazas y las vulnerabilidades de cada sector.

(47) Las evaluaciones de los riesgos de la cadena de suministro, en función de las características del sector afectado, deben tener en cuenta tanto los factores técnicos como, en su caso, los de otra índole, en particular los definidos en la Recomendación (UE) 2019/534, en la evaluación de riesgos coordinada a escala de la UE de la seguridad de las redes 5G y en el conjunto de instrumentos de la UE para la seguridad de las redes 5G acordado por el Grupo de Cooperación. A fin de identificar las cadenas de suministro que deben ser objeto de una evaluación de riesgo coordinada, han de tenerse en cuenta los siguientes criterios: i) la medida en que las entidades esenciales e importantes utilizan servicios, sistemas o productos de TIC críticos y dependen de ellos, ii) la importancia de servicios, sistemas o productos de TIC críticos específicos para desempeñar funciones críticas o sensibles, en particular el tratamiento de datos personales, iii) la disponibilidad de servicios, sistemas o productos de TIC alternativos, iv) la resiliencia de la cadena de suministro global de servicios, sistemas o productos de TIC frente a las perturbaciones, y v) en el caso de los servicios, sistemas o productos de TIC emergentes, el peso que pueden tener en el futuro para las actividades de las entidades.

(48) Con vistas a racionalizar las obligaciones legales impuestas a los proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público y los prestadores de servicios de confianza relacionados con la seguridad de sus redes y sistemas de información, así como para que dichas entidades y sus respectivas autoridades competentes puedan beneficiarse del marco jurídico establecido por la presente Directiva (incluida la designación de un CSIRT responsable de la gestión de riesgos e incidentes, y la participación de las autoridades y los organismos competentes en el trabajo del Grupo de Cooperación y la red de CSIRT), procede incluirlas en el ámbito de aplicación de la presente Directiva. Por consiguiente, es preciso derogar las correspondientes disposiciones establecidas en el

[21] Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G (DO L 88 de 29.3.2019, p. 42.).

Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo[22] y en la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo[23] relativas a la imposición de requisitos de seguridad y notificación a estos tipos de entidades. Las normas sobre las obligaciones de notificación deben entenderse sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo[24].

(49) Cuando proceda, y para evitar perturbaciones innecesarias, las autoridades competentes encargadas de la supervisión y ejecución a efectos de la presente Directiva deben seguir utilizando las directrices nacionales existentes y la legislación nacional adoptada para la transposición de las normas relacionadas con las medidas de seguridad establecidas en el artículo 40, apartado 1, de la Directiva (UE) 2018/1972, así como de los requisitos dispuestos en el artículo 40, apartado 2, de dicha Directiva en cuanto a los parámetros referentes a la importancia de un incidente.

(50) Dada la importancia que están adquiriendo los servicios de comunicaciones interpersonales independientes de la numeración, es necesario garantizar que estos servicios también estén sujetos a requisitos de seguridad apropiados a la vista de su naturaleza específica e importancia económica. Así, los proveedores de este tipo de servicios deben garantizar un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado. Puesto que los proveedores de servicios de comunicaciones interpersonales independientes de la numeración no suelen ejercer un control real sobre la transmisión de las señales a través de las redes, en ciertos sentidos puede considerarse que el grado de riesgo de estos servicios es inferior al de los servicios de comunicaciones electrónicas tradicionales. Lo mismo puede decirse de los servicios de comunicaciones interpersonales que utilizan números y que no ejercen un control real sobre la transmisión de la señal.

(51) Hasta ahora, el mercado interior nunca había dependido tanto del funcionamiento de internet. Los servicios de prácticamente todas las entidades esenciales e importantes dependen de servicios prestados por internet. Para garantizar que la prestación de los servicios suministrados por entidades esenciales e importantes se desarrolle sin problemas, es importante que las redes públicas de comunicaciones electrónicas, tales como las redes troncales de internet o los cables de comunicaciones submarinos, cuenten con medidas de ciberseguridad apropiadas y notifiquen los incidentes en este ámbito.

(52) Cuando corresponda, las entidades deben informar a los destinatarios de su servicio de amenazas concretas y significativas y de las medidas que pueden aplicar para reducir el consiguiente riesgo para ellos mismos. La exigencia de informar a los destinatarios de tales amenazas no exime a las entidades de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para prevenir o subsanar cualquier ciberamenaza y

---

22 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 el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

23 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).

24 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).

restablecer el nivel normal de seguridad del servicio. El suministro de la mencionada información sobre las amenazas de seguridad a los destinatarios debe ser gratuito.

(53) Concretamente, los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público deben informar a los destinatarios del servicio de ciberamenazas concretas y significativas y de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones, por ejemplo, utilizar determinados tipos de soporte lógico o tecnologías de cifrado.

(54) Para salvaguardar la seguridad de las redes y servicios de comunicaciones electrónicas, debe promoverse el uso del cifrado, y en particular el cifrado de extremo a extremo, y, cuando sea necesario, debe ser obligatorio para los proveedores de tales servicios y redes de conformidad con los principios de seguridad y protección de la privacidad por defecto y desde el diseño a efectos del artículo 18. El uso de cifrado de extremo a extremo debe entenderse sin perjuicio de las facultades del Estado miembro para garantizar la protección de sus intereses de seguridad esenciales y la seguridad pública, y para permitir la investigación, detección y enjuiciamiento de infracciones penales con arreglo al Derecho de la Unión. Las soluciones que permitan acceder de manera lícita a la información contenida en comunicaciones cifradas de extremo a extremo deben mantener la eficacia del cifrado en la protección de la privacidad y la seguridad de las comunicaciones, al tiempo que proporcionan una respuesta efectiva a la delincuencia.

(55) La presente Directiva establece un enfoque en dos etapas respecto a la notificación de incidentes a fin de alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a mitigar la posible propagación de incidentes y permita a las entidades buscar apoyo, y, por el otro, una notificación en profundidad que extraiga lecciones valiosas de incidentes individuales y mejore con el tiempo la resiliencia frente a las ciberamenazas de empresas concretas y sectores completos. Cuando las entidades tengan conocimiento de un incidente, deben estar obligadas a presentar una notificación inicial en el plazo de veinticuatro horas, seguida de un informe final a más tardar un mes después. La notificación inicial solo debe incluir la información que sea estrictamente necesaria para que las autoridades competentes tengan constancia del incidente y la entidad pueda solicitar asistencia, en caso de que sea necesario. Cuando proceda, dicha notificación debe indicar si el incidente se debe a una acción presuntamente ilícita o maliciosa. Los Estados miembros deben velar por que el requisito de presentar esta notificación inicial no desvíe los recursos de la entidad notificante de actividades relacionadas con la gestión de incidentes que deban priorizarse. Por otra parte, para evitar que las obligaciones de notificación de incidentes desvíen recursos de la gestión de la respuesta al incidente o puedan comprometer de cualquier otra forma los esfuerzos de las entidades en este sentido, los Estados miembros deben prever también que, en casos debidamente justificados y de acuerdo con las autoridades competentes o el CSIRT, la entidad afectada pueda incumplir los plazos de veinticuatro horas para la notificación inicial y de un mes para el informe final.

(56) Las entidades esenciales e importantes suelen verse en la situación de que un incidente concreto, por sus características, debe notificarse a diversas autoridades en cumplimiento de las obligaciones de notificación recogidas en varios instrumentos jurídicos. Estos casos crean cargas adicionales y también pueden generar inseguridad en cuanto al formato y el procedimiento de tales notificaciones. Por todo ello, y a efectos de simplificar la notificación de los incidentes de seguridad, los Estados miembros deben establecer *un punto de entrada único* para todas las notificaciones

obligatorias en virtud de la presente Directiva y también de otros actos legislativos de la Unión, como el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. La ENISA, en colaboración con el Grupo de Cooperación, debe elaborar modelos de notificación comunes mediante directrices que simplifiquen y racionalicen la información que debe notificarse con arreglo al Derecho de la Unión y reduzcan las cargas para las empresas.

(57) Cuando se sospeche que un incidente guarda relación con actividades delictivas graves en virtud del Derecho de la Unión o nacional, los Estados miembros deben alentar a las entidades esenciales e importantes, sobre la base de las normas aplicables de los procesos penales con arreglo al Derecho de la Unión, a denunciar ante las autoridades policiales competentes los incidentes de naturaleza presuntamente delictiva y grave. Cuando proceda, y sin perjuicio de las normas de protección de datos personales aplicables a Europol, conviene que la EC3 y la ENISA faciliten la coordinación entre las autoridades competentes y las autoridades policiales de distintos Estados miembros.

(58) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes deben cooperar e intercambiar información sobre todas las cuestiones pertinentes con las autoridades de protección de datos y las autoridades de control en virtud de la Directiva 2002/58/CE.

(59) Mantener bases de datos precisas y completas con los nombres de dominio y los datos de registro (los denominado «datos WHOIS») y proporcionar un acceso lícito a tales datos es fundamental para garantizar la seguridad, estabilidad y resiliencia del DNS, lo que a su vez contribuye a garantizar un elevado nivel común de ciberseguridad en el seno de la Unión. Cuando el tratamiento comprenda datos personales, dicho tratamiento debe ajustarse a la legislación de la Unión en materia de protección de datos.

(60) La disponibilidad y accesibilidad oportuna de estos datos para las autoridades públicas, incluidas las autoridades competentes en virtud del Derecho nacional o de la Unión para la prevención, la investigación o el enjuiciamiento de infracciones penales, los CERT, los CSIRT y, por lo que respecta a los datos de sus clientes, los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de ciberseguridad que actúen en nombre de dichos clientes, son fundamentales para evitar y combatir los abusos del sistema de nombres de dominio, en particular para prevenir, detectar y responder a incidentes de ciberseguridad. Dicho acceso debe ser conforme con la legislación de la Unión en materia de protección de datos en la medida en que haya datos personales implicados.

(61) Al objeto de garantizar la disponibilidad de datos precisos y completos sobre el registro de nombres de dominio, los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel (los denominados «registradores») deben recabar y garantizar la integridad y disponibilidad de los datos de registro de nombres de dominio. Concretamente, los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel deben establecer políticas y procedimientos para recoger y mantener datos de registro precisos y completos, así como para prevenir y corregir datos de registro imprecisos con arreglo a las normas de protección de datos de la Unión.

(62) Los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio para ellos deben poner a disposición del público los datos de registro de nombres de dominio que queden fuera del ámbito de aplicación de

las normas de protección de datos de la Unión, como por ejemplo los datos referentes a personas jurídicas[25]. Los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel también deben permitir el acceso lícito a datos específicos sobre el registro de nombres de dominio referentes a personas físicas a solicitantes de acceso legítimos, de conformidad con el Derecho de la Unión en materia de protección de datos. Los Estados miembros deben velar por que los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel para ellos respondan sin demora indebida a las solicitudes de divulgación de datos de registro de nombres de dominio provenientes de solicitantes de acceso legítimos. Los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel para ellos han de establecer políticas y procedimientos para la publicación y divulgación de datos de registro, en particular acuerdos de nivel de servicio para tramitar las solicitudes de acceso de solicitantes de acceso legítimos. El procedimiento de acceso también puede incluir el uso de una interfaz, un portal u otra herramienta técnica que proporcione un sistema eficiente para la solicitud de datos de registro y el acceso a ellos. Con vistas a promover prácticas armonizadas en todo el mercado interior, la Comisión podrá adoptar directrices sobre dichos procedimientos sin perjuicio de las competencias del Comité Europeo de Protección de Datos.

(63) Todas las entidades esenciales e importantes en virtud de la presente Directiva deben estar sometidas a la jurisdicción del Estado miembro en el que prestan sus servicios. Si la entidad presta servicios en más de un Estado miembro, debe estar sometida a la jurisdicción separada y concurrente de cada uno de ellos. Las autoridades competentes de estos Estados miembros deben cooperar, prestarse asistencia mutua y, cuando proceda, emprender medidas conjuntas de supervisión.

(64) A fin de tener en cuenta la naturaleza transfronteriza de los servicios y operaciones de los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de redes de distribución de contenidos, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de servicios digitales, solo un Estado miembro debe tener jurisdicción sobre estas entidades. La jurisdicción debe atribuirse al Estado miembro en el que se encuentre el establecimiento principal en la Unión de la respectiva entidad. El criterio de establecimiento a los efectos de la presente Directiva implica el ejercicio efectivo de una actividad mediante una organización estable. La forma jurídica de dicha organización, ya sea a través de una sucursal o una filial con personalidad jurídica, no es el factor determinante a este respecto. El cumplimiento de este criterio no debe depender de que las redes y sistemas de información se encuentren físicamente en un lugar determinado; la presencia y utilización de tales sistemas no constituyen, por sí mismas, dicho establecimiento principal y, por tanto, no son criterios decisivos para determinar el establecimiento principal. El establecimiento principal debe ser el lugar en el que se toman las decisiones relativas a las medidas para la gestión de riesgos de ciberseguridad dentro de la Unión, que habitualmente coincidirá con el lugar en que se encuentra la administración central de las empresas en la Unión. En caso de que dichas decisiones no se adopten dentro de la Unión, debe considerarse que el establecimiento

[25] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, considerando 14, que dispone que «[e]l presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto».

principal se encuentra en el Estado miembro en el que la entidad tiene el establecimiento con mayor número de trabajadores en la Unión. Cuando los servicios los preste un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial.

(65) En situaciones en las que los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de redes de distribución de contenidos, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de servicios digitales no estén establecidos en la Unión pero ofrezcan servicios dentro de ella, deben designar un representante. Para determinar si dicha entidad ofrece servicios en la Unión, debe averiguarse si hay constancia de que la entidad tiene la intención de ofrecer servicios a personas de uno o varios Estados miembros. La simple accesibilidad en la Unión del sitio web de la entidad o de un intermediario, o de una dirección de correo electrónico y otros datos de contacto, o el empleo de una lengua de uso común en el país tercero en que esté establecida la entidad, no basta para determinar dicha intención. No obstante, factores como el empleo de una lengua o una moneda de uso común en uno o varios Estados miembros, con la posibilidad de encargar servicios en esa otra lengua, o la mención de clientes o usuarios que estén en la Unión, puede revelar que la entidad tiene la intención de ofrecer servicios en la Unión. El representante debe actuar por cuenta de la entidad, y las autoridades competentes o los CSIRT han de poder ponerse en contacto con él. El representante debe haber sido designado expresamente mediante un mandato escrito de la entidad que le autorice para actuar por cuenta de esta en lo que respecta a las obligaciones de la entidad en virtud de la presente Directiva, también por lo que respecta a la notificación de incidentes.

(66) Cuando se intercambie, notifique o comparta de cualquiera forma en virtud de las disposiciones de la presente Directiva información que se considere clasificada de acuerdo con el Derecho nacional o de la Unión, deben aplicarse las correspondientes normas específicas sobre el tratamiento de información clasificada.

(67) Puesto que las ciberamenazas son cada vez más complejas y sofisticadas, el éxito de las medidas de detección y prevención depende en gran medida de que las entidades compartan regularmente información sobre las amenazas y las vulnerabilidades. El intercambio de información contribuye a crear una mayor conciencia sobre las ciberamenazas, lo que a su vez refuerza la capacidad de las entidades para evitar que las amenazas se materialicen en incidentes reales y les permite contener mejor los efectos de los incidentes y recuperarse de manera más eficiente. Ante la ausencia de orientación a nivel de la Unión, son varios los factores que parecen haber dificultado este intercambio de información, en particular la incertidumbre en cuanto a la compatibilidad con las normas sobre competencia y responsabilidad.

(68) Debe animarse a las entidades a aprovechar colectivamente sus conocimientos y experiencias prácticas individuales a nivel estratégico, táctico y operativo para reforzar sus capacidades a fin de evaluar y realizar un seguimiento de las ciberamenazas, defenderse de ellas y reaccionar en consecuencia. Por consiguiente, es necesario propiciar la creación a nivel de la Unión de mecanismos para los acuerdos voluntarios de intercambio de información. Para ello, los Estados miembros también deben apoyar y alentar activamente a las entidades pertinentes que no estén incluidas en el ámbito de aplicación de la presente Directiva para que participen en tales mecanismos de intercambio de información. El funcionamiento de dichos mecanismos debe ajustarse plenamente a las normas en materia de competencia de la Unión, así como a las normas del Derecho de la Unión relativas a la protección de datos.

(69) El tratamiento de datos personales, en la medida en que sea estrictamente necesario y proporcionado a efectos de garantizar la seguridad de las redes y de la información por parte de entidades, autoridades públicas, CERT, CSIRT y proveedores de tecnologías y servicios de seguridad, debe constituir un interés legítimo del responsable del tratamiento de que se trate, tal como se contempla en el Reglamento (UE) 2016/679. Ello debe incluir medidas relacionadas con la prevención, la detección y el análisis de incidentes y la respuesta ante estos, medidas para incrementar el conocimiento relacionado con ciberamenazas específicas, el intercambio de información en el contexto de la corrección y divulgación coordinada de las vulnerabilidades, incluido el intercambio voluntario de información sobre dichos incidentes, así como ciberamenazas y vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración. Dichas medidas pueden requerir el tratamiento de los siguientes tipos de datos personales: direcciones IP, localizadores unificados de recursos (URL), nombres de dominio y direcciones de correo electrónico.

(70) Con vistas a reforzar las facultades y las medidas de supervisión que ayudan a garantizar un cumplimiento efectivo, la presente Directiva debe prever una lista mínima de actuaciones y medios de supervisión a través de los cuales las autoridades competentes puedan supervisar a las entidades esenciales e importantes. Además, la presente Directiva debe establecer una diferenciación respecto al régimen de supervisión entre las entidades esenciales y las entidades importantes con vistas a garantizar un equilibrio justo de las obligaciones para las entidades y las autoridades competentes. En consecuencia, las entidades esenciales deben estar sujetas a un régimen de supervisión completo (*a priori* y *a posteriori*), mientras que las entidades importantes deben estar sujetas a un régimen de supervisión menos estricto exclusivamente *a posteriori*. En este último caso, implica que las entidades importantes no tienen que documentar sistemáticamente la conformidad con los requisitos de gestión de riesgos de ciberseguridad y que las autoridades competentes deben aplicar un enfoque reactivo *a posteriori* respecto a la supervisión y, por ende, no tienen la obligación general de supervisar a dichas entidades.

(71) A fin de garantizar el cumplimiento efectivo, debe fijarse una lista mínima de sanciones administrativas por la infracción de las obligaciones de gestión de riesgos de ciberseguridad y notificación previstas en la presente Directiva, mediante el establecimiento de un marco claro y coherente para tales sanciones en toda la Unión. Debe prestarse la debida atención a la naturaleza, gravedad y duración de la infracción, los perjuicios o las pérdidas reales originados, o los perjuicios o las pérdidas que podrían haberse originado, la intencionalidad o negligencia en la infracción, las medidas adoptadas para prevenir o paliar los perjuicios o las pérdidas sufridos, el grado de responsabilidad o cualquier infracción anterior pertinente. el grado de cooperación con la autoridad competente y cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(72) A fin de garantizar el cumplimiento efectivo de las obligaciones contempladas en la presente Directiva, cada autoridad competente debe estar facultada para imponer multas administrativas o solicitar su imposición.

(73) Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, a la hora de valorar la cuantía apropiada de la multa el nivel la autoridad de supervisión debe tener en cuenta el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. Debe corresponder a los Estados miembros determinar si se debe imponer multas administrativas a las autoridades públicas y en qué medida. La imposición de una multa administrativa no afecta al ejercicio de otras facultades de las autoridades competentes ni a la aplicación de otras sanciones contempladas en las normas nacionales que transpongan la presente Directiva.

(74) Los Estados miembros deben poder establecer las normas sobre las sanciones penales por infracciones de las normas nacionales que transpongan la presente Directiva. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas asociadas no debe entrañar la vulneración del principio *ne bis in idem*, según la interpretación del Tribunal de Justicia.

(75) En los casos en que la presente Directiva no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves de las obligaciones establecidas en la presente Directiva, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(76) Con vistas a reforzar más aun la eficacia y el carácter disuasorio de las sanciones aplicables por la infracción de las obligaciones establecidas en virtud de la presente Directiva, las autoridades competentes deben estar facultadas para aplicar sanciones que consistan en la suspensión de una certificación o autorización referente a una parte o la totalidad de los servicios prestados por una entidad esencial y la imposición de una prohibición temporal de que una persona física ejerza funciones de dirección. Habida cuenta de su gravedad y repercusión en las actividades de las entidades y, en última instancia, en sus consumidores, dichas sanciones deben aplicarse exclusivamente de manera proporcional a la gravedad de la infracción y teniendo en cuenta las circunstancias específicas de cada caso, incluida la intencionalidad o negligencia en la infracción y las medidas adoptadas para prevenir o paliar los daños o perjuicios sufridos. Las sanciones solo deben aplicarse como *ultima ratio*, es decir, únicamente después de haber agotado el resto de medidas de ejecución pertinentes establecidas por la presente Directiva y exclusivamente por el tiempo hasta que las entidades a las que se aplican adopten las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente en nombre de la que se aplicaron dichas sanciones. La imposición de tales sanciones estará sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea, entre ellas el derecho a la tutela judicial efectiva, a la presunción de inocencia y a un proceso con todas las garantías.

(77) La presente Directiva debe establecer normas de cooperación entre las autoridades competentes y las autoridades de control con arreglo al Reglamento (UE) 2016/679 para tratar las infracciones relacionadas con los datos personales.

(78) La presente Directiva debe aspirar a garantizar un nivel elevado de responsabilidad por las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación a nivel de las organizaciones. Por estos motivos, los órganos de dirección

de las entidades incluidas en el ámbito de aplicación de la presente Directiva deben aprobar las medidas de gestión de los riesgos de ciberseguridad y supervisar su aplicación.

(79) Debe introducirse un mecanismo de revisión interpares que permita que los expertos designados por los Estados miembros evalúen la aplicación de las políticas de ciberseguridad, incluido el nivel de capacidades y recursos disponibles de los Estados miembros.

(80) A fin de tener en cuenta ciberamenazas nuevas, la evolución tecnológica o las especificidades sectoriales, procede delegar en la Comisión la facultad de adoptar actos de conformidad con el artículo 290 del TFUE por lo que respecta a los elementos asociados a las medidas de gestión de riesgos requeridas por la presente Directiva. Asimismo, la Comisión debe estar facultada para adoptar actos delegados que establezcan qué categorías de entidades esenciales estarán obligadas a obtener una certificación y en virtud de qué esquemas europeos de certificación de la ciberseguridad específicos. 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 sobre la Mejora de la Legislación de 13 de abril de 2016[26]. 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.

(81) A fin de garantizar condiciones uniformes de ejecución de las disposiciones pertinentes de la presente Directiva sobre las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Cooperación, los elementos técnicos relacionados con las medidas de gestión de riesgos o el tipo de información, el formato y el procedimiento de las notificaciones de los incidentes, 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[27].

(82) La Comisión debe revisar periódicamente lo dispuesto en la presente Directiva, en consulta con las partes interesadas, en particular para determinar si se precisa alguna modificación a raíz de cambios en la situación social, política, de la tecnología o el mercado.

(83) Dado que el objetivo de la presente Directiva, a saber, garantizar un elevado nivel común de ciberseguridad en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a los efectos 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.

---

[26] DO L 123 de 12.5.2016, p. 1.

[27] 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).

(84) La presente Directiva observa los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído. La presente Directiva debe aplicarse con arreglo a esos derechos y principios.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

1. La presente Directiva establece medidas destinadas a garantizar un elevado nivel común de ciberseguridad dentro de la Unión.

2. A tal fin, la presente Directiva:

   a) establece obligaciones por las cuales los Estados miembros deben adoptar estrategias nacionales de ciberseguridad y designar autoridades nacionales competentes, puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT);

   b) establece obligaciones de gestión de riesgos de ciberseguridad y notificación para las entidades cuyo tipo se enmarca en el de las entidades esenciales del anexo I y en el de las entidades importantes del anexo II; y

   c) contempla obligaciones relativas al intercambio de información sobre ciberseguridad.

Artículo 2

Ámbito de aplicación

1. La presente Directiva se aplicará a las entidades públicas y privadas cuyo tipo se enmarque en el de las entidades esenciales del anexo I y en el de las entidades importantes del anexo II. La presente Directiva no se aplicará a las entidades que se consideren microempresas o pequeñas empresas en el sentido de la Recomendación 2003/361/CE de la Comisión[28].

2. No obstante lo dispuesto, independientemente de su tamaño, la presente Directiva también se aplicará a las entidades contempladas en los anexos I y II cuando:

[28] 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).

a) los servicios sean prestados por una de las siguientes entidades:

i) redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público a que se refiere el anexo I, punto 8,

ii) prestadores de servicios de confianza a que se refiere el anexo I, punto 8,

iii) registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio (DNS) a que se refiere el anexo I, punto 8,

b) la entidad sea una entidad de la Administración pública tal como se define en el artículo 4, punto 23;

c) la entidad sea el único proveedor de un servicio en un Estado miembro;

d) una posible perturbación del servicio prestado por la entidad pudiera tener repercusiones sobre la seguridad pública, el orden público o la salud pública;

e) una posible perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;

f) la entidad sea crítica a la luz de su importancia específica a nivel regional o nacional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro;

g) la entidad se identifique como entidad crítica en virtud de la Directiva (UE) XXXX/XXXX del Parlamento Europeo y del Consejo[29] [Directiva sobre la resiliencia de las entidades críticas] o como una entidad equivalente a una entidad crítica con arreglo al artículo 7 de dicha Directiva.

Los Estados miembros establecerán una lista de las entidades identificadas al amparo de las letras b) a f) y la presentarán a la Comisión en el plazo de [seis meses después del plazo de transposición]. Posteriormente, los Estados miembros revisarán periódicamente la lista, al menos cada dos años, y la actualizarán cuando proceda.

3. La presente Directiva se entenderá sin perjuicio de las competencias de los Estados miembros relativas al mantenimiento de la seguridad pública, la defensa y la seguridad nacional de conformidad con el Derecho de la Unión.

4. La presente Directiva se entenderá sin perjuicio de la Directiva 2008/114/CE del Consejo[30] y las Directivas 2011/93/UE[31] y 2013/40/UE[32] del Parlamento Europeo y del Consejo.

5. Sin perjuicio de lo dispuesto en el artículo 346 del TFUE, la información que se considere confidencial de acuerdo con las normas de la Unión y nacionales, como las

---

29 *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

30 Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

31 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).

32 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DO L 218 de 14.8.2013, p. 8).

normas sobre confidencialidad empresarial, se intercambiará con la Comisión y otras autoridades competentes únicamente cuando tal intercambio sea necesario a efectos de la aplicación de la presente Directiva. La información que se intercambie se limitará a aquella que resulte pertinente y proporcionada para la finalidad del intercambio. El intercambio de información preservará la confidencialidad de esta y protegerá la seguridad y los intereses comerciales de las entidades esenciales o importantes.

6. Cuando las disposiciones de un acto jurídico de la Unión de carácter sectorial exijan que las entidades esenciales o importantes adopten medidas para la gestión de riesgos de ciberseguridad o notifiquen los incidentes o las ciberamenazas significativas y dichos requisitos tengan un efecto al menos equivalente al de las obligaciones establecidas en la presente Directiva, no se aplicarán las disposiciones pertinentes de la presente Directiva, incluidas las relativas a la supervisión y la ejecución recogidas en el capítulo VI.

Artículo 3

Armonización mínima

Sin perjuicio del resto de sus obligaciones en virtud del Derecho de la Unión, los Estados miembros podrán, de conformidad con la presente Directiva, adoptar o mantener disposiciones que garanticen un nivel más elevado de ciberseguridad.

Artículo 4

Definiciones

A los efectos de la presente Directiva, se entenderá por:

1) «redes y sistemas de información»:

   a) una red de comunicaciones electrónicas en el sentido del artículo 2, punto 1, de la Directiva (UE) 2018/1972;

   b) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales;

   c) los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

2) «seguridad de las redes y sistemas de información»: la capacidad de las redes y los sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

3) «ciberseguridad»: ciberseguridad en el sentido del artículo 2, punto 1, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[33];

4) «estrategia nacional de ciberseguridad»: marco coherente de un Estado miembro que establece prioridades y objetivos estratégicos de seguridad de las redes y sistemas de información en dicho Estado miembro;

5) «incidente»: todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por redes y sistemas de información o accesibles a través de ellos;

6) «gestión de incidentes»: conjunto de medidas y procedimientos destinados a detectar, analizar y limitar un incidente y responder ante este;

7) «ciberamenaza»: una ciberamenaza en el sentido del artículo 2, punto 8, del Reglamento (UE) 2019/881;

8) «vulnerabilidad»: deficiencia, susceptibilidad o fallo de un activo, sistema, proceso o control que puede ser aprovechado por una ciberamenaza;

9) «representante»: toda persona física o jurídica establecida en la Unión que ha sido designada expresamente para actuar por cuenta de i) un proveedor de servicios de DNS, un registro de nombres de dominio de primer nivel, un proveedor de servicios de computación en nube, un proveedor de servicios de centro de datos o un proveedor de redes de distribución de contenidos contemplado en el anexo I, punto 8, o de ii) entidades contempladas en el anexo II, punto 6, que no estén establecidas en la Unión, a las que puede dirigirse una autoridad competente nacional o un CSIRT en sustitución de la entidad, en lo que respecta a las obligaciones de dicha entidad en virtud de la presente Directiva;

10) «norma»: una norma en el sentido del artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[34];

11) «especificación técnica»: una especificación técnica en el sentido del artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012;

12) «punto de intercambio de internet (IXP)»: una instalación de la red que permite interconectar más de dos redes independientes (sistemas autónomos), principalmente para facilitar el intercambio de tráfico de internet; un IXP solo permite interconectar sistemas autónomos; un IXP no requiere que el tráfico de internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, no modifica dicho tráfico ni interfiere de otra forma en el mismo;

---

33 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad) (DO L 151 de 7.6.2019, p. 15).

34 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).

13) «sistema de nombres de dominio (DNS)»: un sistema de nombres distribuido jerárquicamente que permite a los usuarios finales acceder a los servicios y recursos de internet;

14) «proveedor de servicios de DNS»: una entidad que presta servicios de resolución recursiva o autoritativa de nombres de dominio a los usuarios finales de internet y a otros proveedores de servicios de DNS;

15) «registro de nombres de dominio de primer nivel»: una entidad en la que se ha delegado un dominio de primer nivel específico y que es responsable de administrar dicho dominio, incluido el registro de nombres de dominio en el dominio de primer nivel y el funcionamiento técnico del dominio de primer nivel, en particular la explotación de sus servidores de nombre, el mantenimiento de sus bases de datos y la distribución de los archivos de zona del dominio de primer nivel entre los servidores de nombre;

16) «servicio digital»: un servicio en el sentido del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo[35];

17) «mercado en línea»: un servicio digital en el sentido del artículo 2, letra n), de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo[36];

18) «motor de búsqueda en línea»: un servicio digital en el sentido del artículo 2, punto 5, del Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo[37];

19) «servicio de computación en nube»: un servicio digital que hace posible la administración bajo demanda y el acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos distribuidos que se pueden compartir;

20) «servicio de centro de datos»: un servicio que engloba las estructuras, o agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de las tecnologías de la información y los equipos de red que proporcionan servicios de almacenamiento, tratamiento y transporte de datos, junto con todas las instalaciones e infraestructuras necesarias para la distribución de la energía y el control ambiental;

21) «red de distribución de contenidos»: una red de servidores distribuidos geográficamente a efectos de garantizar una elevada disponibilidad, accesibilidad o distribución rápida de contenidos y servicios digitales a los usuarios de internet en nombre de los proveedores de contenidos y servicios;

22) «plataforma de servicios de redes sociales»: una plataforma que permite que los usuarios finales se conecten, compartan, descubran y se comuniquen entre sí a través

---

35 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 (DO L 241 de 17.9.2015, p. 1).

36 Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») (DO L 149 de 11.6.2005, p. 22).

37 Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para las empresas que utilizan servicios de intermediación en línea (DO L 186 de 11.7.2019, p. 57).

de múltiples dispositivos y, en particular, mediante chats, publicaciones, vídeos y recomendaciones;

23) «entidad de la Administración pública»: una entidad de un Estado miembro que cumple los siguientes criterios:

a) se ha creado para satisfacer necesidades de interés general y no tiene carácter industrial o mercantil;

b) está dotada de personalidad jurídica;

c) está mayoritariamente financiada por el Estado, la autoridad regional u otras entidades de Derecho público; o bien, cuya gestión se halla sometida a un control por parte de estas autoridades o entidades; o cuyos órganos de administración, de dirección o de supervisión están compuestos por miembros más de la mitad de los cuales sean nombrados por el Estado, la autoridad regional u otras entidades de Derecho público;

d) tiene facultad para dirigir a las personas físicas o jurídicas resoluciones administrativas o reglamentarias que afectan a sus derechos en la circulación transfronteriza de personas, bienes, servicios o capital.

Quedan excluidas las entidades de la Administración pública que realizan actividades en los ámbitos de la seguridad pública, la policía, la defensa o la seguridad nacional.

24) «entidad»: toda persona física o jurídica constituida y reconocida como tal en virtud del Derecho nacional de su lugar de establecimiento y que, actuando en nombre propio, puede ejercer derechos y estar sujeta a obligaciones;

25) «entidad esencial»: toda entidad cuyo tipo se enmarca en el de las entidades esenciales del anexo I;

26) «entidad importante»: toda entidad cuyo tipo se enmarca en el de las entidades importantes del anexo II;

CAPÍTULO II

Marcos reglamentarios de ciberseguridad coordinados

Artículo 5
Estrategia nacional de ciberseguridad

1. Cada Estado miembro adoptará una estrategia nacional de ciberseguridad en la que se establecerán los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad. La estrategia nacional de ciberseguridad incluirá, en particular, los aspectos siguientes:

a) una definición de los objetivos y las prioridades de la estrategia de ciberseguridad de los Estados miembros;

b) un marco de gobernanza para lograr dichos objetivos y prioridades, incluidas las políticas a que se refiere el apartado 2 y las funciones y responsabilidades de las entidades y los organismos públicos y de los demás actores pertinentes;

c) una evaluación para determinar los activos pertinentes y los riesgos de ciberseguridad en ese Estado miembro;

d) una determinación de las medidas para garantizar la preparación, respuesta y recuperación frente a incidentes, incluida la cooperación entre los sectores público y privado;

e) una lista de los diversos actores y autoridades que participan en la ejecución de la estrategia nacional de ciberseguridad;

f) un marco político para la coordinación reforzada entre las autoridades competentes en virtud de la presente Directiva y la Directiva (UE) XXXX/XXXX del Parlamento Europeo y del Consejo[38] [Directiva sobre la resiliencia de las entidades críticas] a efectos del intercambio de información sobre incidentes y ciberamenazas y el ejercicio de las tareas de supervisión.

2. En el marco de la estrategia nacional de ciberseguridad, los Estados miembros adoptarán, en particular, las siguientes políticas:

a) una política para abordar la ciberseguridad en la cadena de suministro de productos y servicios de TIC utilizados por las entidades esenciales e importantes para la prestación de sus servicios;

b) directrices relativas a la inclusión y especificación de los requisitos en materia de ciberseguridad aplicables a los productos y servicios de TIC en la contratación pública;

c) una política para promover y facilitar una divulgación coordinada de las vulnerabilidades en el sentido del artículo 6;

d) una política orientada a mantener la disponibilidad general y la integridad del núcleo público de la internet abierta;

e) una política sobre la promoción y el desarrollo de capacidades de ciberseguridad, concienciación e iniciativas de investigación y desarrollo;

f) una política destinada a prestar apoyo a las instituciones académicas y de investigación para que desarrollen herramientas de ciberseguridad e infraestructuras de red seguras;

g) una política, los procedimientos pertinentes y las herramientas apropiadas para compartir información en apoyo del intercambio voluntario de información sobre ciberseguridad entre las empresas, con arreglo al Derecho de la Unión;

h) una política que atienda a las necesidades específicas de las pymes, especialmente de las excluidas del ámbito de aplicación de la presente Directiva, por lo que respecta a orientaciones y apoyo para mejorar su resiliencia frente a las amenazas de ciberseguridad.

3. Los Estados miembros notificarán sus estrategias nacionales de ciberseguridad a la Comisión en el plazo de tres meses a partir de su adopción. Los Estados miembros podrán excluir información específica de la notificación cuando y en la medida en que sea estrictamente necesario para preservar la seguridad nacional.

4. Los Estados miembros evaluarán sus estrategias nacionales de ciberseguridad al menos cada cuatro años en función de unos indicadores de rendimiento clave y las modificarán cuando proceda. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) prestará asistencia a los Estados miembros, cuando así lo

[38] *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

soliciten, a la hora de elaborar una estrategia nacional y los indicadores de rendimiento clave para su evaluación.

Artículo 6

Divulgación coordinada de las vulnerabilidades y un Registro Europeo de Vulnerabilidades

1. Cada Estado miembros designará a uno de sus CSIRT referidos en el artículo 9 como coordinador a efectos de la divulgación coordinada de las vulnerabilidades. El CSIRT designado ejercerá de intermediario de confianza y facilitará, cuando sea necesario, la interacción entre la entidad notificante y el fabricante o proveedor de productos o servicios de TIC. Cuando la vulnerabilidad notificada afecte a varios fabricantes o proveedores de productos o servicios de TIC de la Unión, el CSIRT designado de cada Estado miembro afectado cooperará con la red de CSIRT.

2. La ENISA desarrollará y mantendrá un Registro Europeo de Vulnerabilidades. Para ello, la Agencia establecerá y mantendrá los sistemas de información, las políticas y los procedimientos apropiados con vistas, en particular, a permitir que las entidades importantes y esenciales y sus proveedores de redes y sistemas de información divulguen y registren vulnerabilidades presentes en los productos o servicios de TIC, así como a facilitar a todas las partes interesadas acceso a la información sobre las vulnerabilidades que figura en el registro. Concretamente, el registro incluirá información que describa la vulnerabilidad, los productos o servicios de TIC afectados y la gravedad de la vulnerabilidad por lo que respecta a las circunstancias en que puede explotarse, la disponibilidad de los parches de seguridad asociados y, a falta de ellos, orientaciones dirigidas a los usuarios de productos y servicios vulnerables sobre la forma de reducir los riesgos derivados de las vulnerabilidades reveladas.

Artículo 7

Marcos nacionales de gestión de crisis de ciberseguridad

1. Cada Estado miembro designará una o varias autoridades competentes responsables de la gestión de incidentes y crisis a gran escala. Los Estados miembros velarán por que las autoridades competentes dispongan de los recursos adecuados para ejercer las tareas que les son asignadas de forma efectiva y eficiente.

2. Cada Estado miembro determinará las capacidades, los activos y los procedimientos que se pueden desplegar en caso de que se produzca una crisis a los efectos de la presente Directiva.

3. Cada Estado miembro adoptará un plan nacional de respuesta a incidentes y crisis de ciberseguridad en el que se fijen los objetivos y las modalidades de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. El plan establecerá, en particular, los siguientes aspectos:

   a) los objetivos de las medidas y actividades nacionales en materia de preparación;

   b) las tareas y responsabilidades de las autoridades nacionales competentes;

c) los procedimientos de gestión de crisis y los canales para el intercambio de información;

d) las medidas de preparación, incluidos los ejercicios y las actividades de formación;

e) las partes interesadas pertinentes, tanto públicas como privadas, y la infraestructura implicada;

f) los procedimientos y mecanismos nacionales entre las autoridades y los organismos nacionales pertinentes para garantizar la participación efectiva del Estado miembro en la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel de la Unión y el respaldo de ella.

4. Los Estados miembros comunicarán a la Comisión la designación de sus autoridades competentes referidas en el apartado 1 y presentarán sus planes nacionales de respuesta a incidentes y crisis de ciberseguridad contemplados en el apartado 3 en el plazo de tres meses a partir de tal designación y la adopción de dichos planes. Los Estados miembros podrán excluir información específica del plan cuando y en la medida en que sea estrictamente necesario para su seguridad nacional.

Artículo 8

Autoridades nacionales competentes y puntos de contacto únicos

1. Cada Estado miembro designará una o más autoridades competentes encargadas de la ciberseguridad y de las tareas de supervisión a que se refiere el capítulo VI de la presente Directiva. Los Estados miembros podrán designar a tales efectos una autoridad o autoridades existentes.

2. Las autoridades competentes a que se refiere el apartado 1 supervisarán la aplicación de la presente Directiva a escala nacional.

3. Cada Estado miembro designará un punto de contacto único en materia de ciberseguridad (en lo sucesivo, «punto de contacto único»). Si un Estado miembro designa únicamente una autoridad competente, dicha autoridad también será el punto de contacto único correspondiente a dicho Estado miembro.

4. Cada punto de contacto único ejercerá una función de enlace para garantizar la cooperación transfronteriza de las autoridades de su Estado miembro con las autoridades competentes en otros Estados miembros, así como para garantizar la cooperación intersectorial con otras autoridades nacionales competentes dentro de su Estado miembro.

5. Los Estados miembros velarán por que las autoridades competentes a que se refiere el apartado 1 y los puntos de contacto únicos dispongan de recursos adecuados para ejercer las funciones que les son asignadas de forma efectiva y eficiente y cumplir así los objetivos de la presente Directiva. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de los representantes designados en el Grupo de cooperación a que se refiere el artículo 12.

6. Los Estados miembros notificarán sin dilación indebida a la Comisión la autoridad competente a que se refiere el apartado 1 y el punto de contacto único contemplado en el apartado 3 que hayan designado, sus tareas y cualquier cambio posterior que se

introduzca. Cada Estado miembro hará pública su designación. La Comisión publicará la lista de puntos de contacto únicos designados.

Artículo 9

Equipos de respuesta a incidentes de seguridad informática (CSIRT)

1. Cada Estado miembro designará uno o varios CSIRT que cumplirán los requisitos establecidos en el artículo 10, apartado 1, que cubran al menos los sectores, subsectores o entidades que figuran en los anexos I y II y se responsabilicen de la gestión de incidentes de conformidad con un procedimiento claramente definido. Podrá crearse un CSIRT en el marco de una autoridad competente a que se refiere el artículo 8.
2. Los Estados miembros velarán por que cada CSIRT disponga de los recursos adecuados para llevar a cabo eficazmente sus tareas, tal como se establece en el artículo 10, apartado 2.
3. Los Estados miembros velarán por que cada CSIRT tenga a su disposición una infraestructura de comunicación e información apropiada, segura y resiliente para intercambiar información con las entidades esenciales e importantes y otras partes interesadas pertinentes. Para ello, los Estados miembros se asegurarán de que los CSIRT contribuyan al despliegue de herramientas seguras para el intercambio de información.
4. Los CSIRT cooperarán y, cuando proceda, intercambiarán información pertinente de conformidad con el artículo 26 con comunidades sectoriales o intersectoriales de entidades esenciales e importantes de confianza.
5. Los CSIRT participarán en las revisiones interpares organizadas con arreglo al artículo 16.
6. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT a que se refiere el artículo 13.
7. Los Estados miembros comunicarán a la Comisión sin demora indebida los CSIRT designados de conformidad con el apartado 1, el CSIRT coordinador designado con arreglo al artículo 6, apartado 1, y sus respectivas tareas desempeñadas en relación con las entidades contempladas en los anexos I y II.
8. Los Estados miembros podrán solicitar la asistencia de la ENISA a la hora de crear CSIRT nacionales.

Artículo 10

Obligaciones y tareas de los CSIRT

1. Los CSIRT cumplirán las siguientes obligaciones:
   a) los CSIRT garantizarán una gran disponibilidad de sus servicios de comunicaciones evitando los fallos puntuales simples y contarán con varios medios para ser contactado y contactar con otros en todo momento. Los CSIRT especificarán claramente los canales de comunicación y los darán a conocer a los grupos de usuarios y los socios colaboradores;

b) las dependencias de los CSIRT y los sistemas de información de apoyo estarán situados en lugares seguros;

c) los CSIRT estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes, en particular, con el fin de facilitar la efectividad y eficiencia de los traspasos;

d) los CSIRT contarán con personal suficiente para garantizar su disponibilidad en todo momento;

e) los CSIRT estarán dotados de sistemas redundantes y espacios de trabajo de reserva para garantizar la continuidad de sus servicios;

f) los CSIRT podrán participar en redes de cooperación internacional.

2. Las tareas de los CSIRT serán las siguientes:

a) supervisar las ciberamenazas, las vulnerabilidades y los incidentes a escala nacional;

b) difundir alertas tempranas, alertas, avisos e información sobre las ciberamenazas, las vulnerabilidades y los incidentes entre las entidades esenciales e importantes y otras partes interesadas pertinentes;

c) responder a incidentes;

d) efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación en materia de ciberseguridad;

e) llevar a cabo, a petición de una entidad, una exploración proactiva de las redes y los sistemas de información utilizados para la prestación de sus servicios;

f) participar en la red de CSIRT y prestar asistencia mutua a otros miembros de la red cuando la soliciten.

3. Los CSIRT establecerán relaciones de cooperación con actores pertinentes del sector privado, con vistas a mejorar la consecución de los objetivos de la Directiva.

4. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas, sistemas de clasificación y taxonomías en relación con los siguientes aspectos:

a) los procedimientos de gestión de incidentes;

b) la gestión de crisis de ciberseguridad;

c) la divulgación coordinada de las vulnerabilidades.

Artículo 11

Cooperación a escala nacional

1. Cuando sean distintos, las autoridades competentes referidas en el artículo 8, el punto de contacto único y los CSIRT del mismo Estado miembro cooperarán entre sí respecto al cumplimiento de las obligaciones establecidas en la presente Directiva.

2. Los Estados miembros velarán por que sus autoridades competentes o sus CSIRT reciban las notificaciones sobre los incidentes y los cuasiincidentes y ciberamenazas significativos presentadas en el marco de la presente Directiva. Cuando un Estado miembro decida que sus CSIRT no recibirán dichas notificaciones, se dará a estos

últimos, en la medida necesaria para que lleven a cabo sus tareas, el acceso a los datos sobre incidentes notificados por las entidades esenciales o importantes, con arreglo al artículo 20.

3. Cada Estado miembro velará por que sus autoridades competentes o los CSIRT informen a su punto de contacto único sobre las notificaciones de incidentes, y cuasiincidentes y ciberamenazas significativos presentadas en el marco de la presente Directiva.

4. En la medida necesaria para cumplir de manera efectiva las tareas y las obligaciones establecidas en la presente Directiva, los Estados miembros garantizarán una cooperación apropiada entre las autoridades competentes y los puntos de contacto únicos y las autoridades policiales, las autoridades de protección de datos y las autoridades responsables de infraestructuras críticas con arreglo a la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas], así como las autoridades financieras nacionales designadas de conformidad con el Reglamento (UE) XXXX/XXXX del Parlamento Europeo y del Consejo[39] [Reglamento sobre la resiliencia operativa digital del sector financiero] dentro de dicho Estado miembro.

5. Los Estados miembros velarán por que sus autoridades competentes faciliten periódicamente información a las autoridades competentes designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] sobre los riesgos de ciberseguridad, las ciberamenazas y los incidentes que afecten a entidades esenciales identificadas como críticas, o como entidades equivalentes a entidades críticas, con arreglo a dicha Directiva, así como las medidas adoptadas por las autoridades competentes en respuesta a estos riesgos e incidentes.

CAPÍTULO III

Cooperación

Artículo 12
Grupo de Cooperación

1. Se establece un Grupo de Cooperación a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros en el ámbito de aplicación de la Directiva.

2. El Grupo de Cooperación llevará a cabo sus tareas con arreglo a los programas de trabajo bienales a que se refiere el apartado 6.

3. El Grupo de Cooperación estará formado por representantes de los Estados miembros, la Comisión y la ENISA. El Servicio Europeo de Acción Exterior participará en las actividades del Grupo de Cooperación en calidad de observador. Las Autoridades Europeas de Supervisión (AES) con arreglo a lo dispuesto en el artículo 17, apartado 5, letra c), del Reglamento (UE) XXXX/XXXX [Reglamento sobre la resiliencia operativa digital del sector financiero] podrán participar en las actividades del Grupo de Cooperación.

[39] *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

Cuando proceda, el Grupo de Cooperación podrá invitar a representantes de las partes interesadas pertinentes a que participen en su labor.

La Comisión se hará cargo de la secretaría.

4. El Grupo de Cooperación llevará a cabo las siguientes tareas:

   a) proporcionar orientación a las autoridades competentes en relación con la transposición y aplicación de la presente Directiva;

   b) intercambiar buenas prácticas e información en relación con la aplicación de la presente Directiva, también por lo que respecta a las ciberamenazas, los incidentes, las vulnerabilidades, los cuasiincidentes, las iniciativas de concienciación, las formaciones, los ejercicios y las habilidades, el desarrollo de capacidades, así como las normas y especificaciones técnicas;

   c) intercambiar recomendaciones y cooperar con la Comisión en iniciativas políticas sobre aspectos emergentes de la ciberseguridad;

   d) intercambiar recomendaciones y cooperar con la Comisión en la redacción de los actos delegados o de ejecución que adopte en virtud de la presente Directiva;

   e) intercambiar buenas prácticas e información con las instituciones, los órganos y los organismos de la Unión pertinentes;

   f) analizar los informes sobre la revisión interpares a que se refiere el artículo 16, apartado 7;

   g) analizar los resultados de las actividades conjuntas de supervisión en casos transfronterizos, tal como se contempla en el artículo 34;

   h) proporcionar orientación estratégica a la red de CSIRT sobre cuestiones emergentes específicas;

   i) contribuir a las capacidades de ciberseguridad de toda la Unión facilitando el intercambio de funcionarios nacionales a través de un programa de desarrollo de capacidades en el que participe el personal de las autoridades competentes o los CSIRT de los Estados miembros;

   j) organizar reuniones conjuntas periódicas con las partes interesadas privadas pertinentes de toda la Unión para tratar las actividades realizadas por el Grupo y recabar apreciaciones sobre los desafíos políticos emergentes;

   k) debatir sobre las labores realizadas en relación con los ejercicios de ciberseguridad, incluida la labor efectuada por la ENISA.

5. El Grupo de Cooperación podrá solicitar a la red de CSIRT un informe técnico sobre temas concretos.

6. A más tardar el … [veinticuatro meses después de la fecha de entrada en vigor de la presente Directiva], y cada dos años a partir de entonces, el Grupo de cooperación establecerá un programa de trabajo sobre las acciones que deben emprenderse para alcanzar sus objetivos y llevar a cabo sus tareas. El calendario del primer programa adoptado en virtud de la presente Directiva se adecuará al del último programa adoptado con arreglo a la Directiva (UE) 2016/1148.

7. La Comisión podrá adoptar actos de ejecución para establecer las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Cooperación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 37, apartado 2.

8. El Grupo de Cooperación se reunirá periódicamente, y por lo menos una vez al año, con el Grupo de resiliencia de las entidades críticas establecido en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] para promover la cooperación estratégica y el intercambio de información.

Artículo 13
Red de CSIRT

1. Con vistas a contribuir al refuerzo de la confianza y la seguridad y la promoción de una cooperación operativa rápida y eficaz entre los Estados miembros, se establece una red de CSIRT nacionales.

2. La red de CSIRT estará formada por representantes de los CSIRT de los Estados miembros y el CERT-EU. La Comisión participará en la red de CSIRT en calidad de observador. La ENISA se hará cargo de la secretaría y apoyará activamente la cooperación entre los CSIRT.

3. La red de CSIRT llevará a cabo las siguientes tareas:

   a) intercambiar información sobre las capacidades de los CSIRT;

   b) intercambiar información pertinente sobre los incidentes, los cuasiincidentes, las ciberamenazas, los riesgos y las vulnerabilidades;

   c) a instancias de un representante de la red de CSIRT que pueda verse afectado por un incidente, intercambiar y debatir información relacionada con ese incidente y las ciberamenazas, los riesgos y las vulnerabilidades asociados;

   d) a instancias de un representante de la red de CSIRT, debatir y, cuando sea posible, aplicar una respuesta coordinada a un incidente que se haya detectado dentro del ámbito de competencias de ese Estado miembro;

   e) prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos con arreglo a la presente Directiva;

   f) cooperar y prestar asistencia a los CSIRT designados a que se refiere el artículo 6 por lo que respecta a la gestión de la divulgación coordinada de las vulnerabilidades con múltiples interesados que afecten a varios fabricantes o proveedores de productos, servicios y procesos de TIC establecidos en distintos Estados miembros;

   g) debatir e identificar más formas de cooperación operativa, incluidas las relacionadas con:

      i) las categorías de ciberamenazas e incidentes,

      ii) las alertas tempranas,

      iii) la asistencia mutua,

      iv) los principios y las modalidades de coordinación en respuesta a riesgos e incidentes transfronterizos,

v) la contribución al plan nacional de respuesta a incidentes y crisis de ciberseguridad a que se refiere el artículo 7, apartado 3;

h) informar al Grupo de Cooperación sobre sus actividades y sobre las formas adicionales de cooperación operativa sobre las que se haya discutido conforme a la letra g), y solicitar, cuando sea necesario, directrices a este respecto;

i) hacer balance de los ejercicios de ciberseguridad, también de los organizados por la ENISA;

j) a instancias de un CSIRT determinado, analizar las capacidades y la preparación de dicho CSIRT;

k) cooperar e intercambiar información con los centros de operaciones de seguridad (COS) regionales y a escala de la Unión para mejorar el conocimiento común de la situación relativa a los incidentes y las amenazas en toda la Unión;

l) analizar los informes sobre la revisión interpares a que se refiere el artículo 16, apartado 7;

m) publicar directrices para facilitar la convergencia de las prácticas operativas con respecto a la aplicación de lo dispuesto en el presente artículo en lo que atañe a la cooperación operativa.

4. A efectos de la revisión a que se refiere el artículo 35, a más tardar el [veinticuatro meses después de la fecha de entrada en vigor de la presente Directiva], y cada dos años a partir de entonces, la red de CSIRT evaluará los progresos realizados en el ámbito de la cooperación operativa y elaborará un informe. Concretamente, el informe extraerá conclusiones sobre los resultados de las revisiones interpares a que se refiere el artículo 16 realizadas en relación con los CSIRT nacionales, en particular las conclusiones y recomendaciones, practicadas con arreglo al presente artículo. Dicho informe también se enviará al Grupo de Cooperación.

5. La red de CSIRT adoptará su reglamento interno.

Artículo 14

Red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe)

1. De cara a respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio regular de información entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión, se crea la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe).

2. EU-CyCLONe estará formada por representantes de las autoridades de gestión de crisis de los Estados miembros designadas con arreglo al artículo 7, la Comisión y la ENISA. La ENISA se hará cargo de la secretaría de la red y promoverá el intercambio seguro de información.

3. Las tareas de EU-CyCLONe serán las siguientes:

a) incrementar el nivel de preparación para la gestión de incidentes y crisis a gran escala;

b) desarrollar una conciencia situacional conjunta de los sucesos de ciberseguridad pertinentes;

c) coordinar la gestión de incidentes y crisis a gran escala y contribuir a la toma de decisiones a nivel político en relación con tales incidentes y crisis;

d) examinar los planes nacionales de respuesta a incidentes y crisis de ciberseguridad a que se refiere el artículo 7, apartado 2.

4. EU-CyCLONe adoptará su reglamento interno.

5. EU-CyCLONe informará periódicamente al Grupo de Cooperación de las ciberamenazas, los incidentes y las tendencias, con atención especial a las correspondientes repercusiones para las entidades esenciales e importantes.

6. EU-CyCLONe cooperará con la red de CSIRT sobre la base de disposiciones de procedimiento acordadas.

Artículo 15

Informe sobre la situación de la ciberseguridad en la Unión

1. La ENISA publicará, en cooperación con la Comisión, un informe bienal sobre la situación de la ciberseguridad en la Unión. En el informe se recogerá, en particular, una evaluación de los siguientes aspectos:

a) la evolución de las capacidades de ciberseguridad en toda la Unión;

b) los recursos técnicos, financieros y humanos a disposición de las autoridades competentes y las políticas de ciberseguridad, y la aplicación de las medidas de supervisión y de ejecución a la luz de los resultados de las revisiones interpares contempladas en el artículo 16;

c) un índice de ciberseguridad que proporcione una evaluación agregada del nivel de madurez de las capacidades de ciberseguridad.

2. El informe incluirá recomendaciones políticas concretas para incrementar el nivel de ciberseguridad en toda la Unión y un resumen de las conclusiones correspondientes al período de que se trate de los informes sobre la situación técnica de la ciberseguridad en la UE publicados por la ENISA de conformidad con el artículo 7, apartado 6, del Reglamento (UE) 2019/881.

Artículo 16

Revisiones interpares

1. A más tardar dieciocho meses después de la entrada en vigor de la presente Directiva, la Comisión establecerá, tras consultar al Grupo de Cooperación y a la ENISA, la metodología y el contenido de un sistema de revisión interpares para evaluar la eficacia de las políticas de ciberseguridad de los Estados miembros. Las revisiones serán realizadas por expertos técnicos en ciberseguridad procedentes de Estados miembros que no sean el examinado y abarcarán, por lo menos, los siguientes aspectos:

i) la eficacia de la aplicación de los requisitos de gestión de riesgos de ciberseguridad y las obligaciones de notificación a que se refieren los artículos 18 y 20;

ii) el nivel de capacidades, incluidos los recursos financieros, técnicos y humanos disponibles, y la eficacia con que las autoridades nacionales competentes han llevado a cabo sus tareas;

iii) las capacidades operativas y la eficacia de los CSIRT;

iv) la eficacia de la asistencia mutua a que se refiere el artículo 34;

v) la eficacia del marco para el intercambio de información a que se refiere el artículo 26 de la presente Directiva.

2. La metodología abarcará criterios objetivos, no discriminatorios, justos y transparentes que los Estados miembros utilizarán para designar los expertos elegibles para realizar las revisiones interpares. La ENISA y la Comisión designarán expertos para que participen en las revisiones interpares en calidad de observadores. La Comisión, con el apoyo de la ENISA, establecerá dentro de la metodología referida en el apartado 1 un sistema objetivo, no discriminatorio, justo y transparente para la selección y la asignación aleatoria de expertos a cada revisión interpares.

3. Los aspectos organizativos de las revisiones interpares serán decididos por la Comisión, con el apoyo de la ENISA, y se basarán, previa consulta con el Grupo de Cooperación, en los criterios definidos en la metodología a que se refiere el apartado 1. Las revisiones interpares evaluarán los aspectos mencionados en el apartado 1 respecto a todos los Estados miembros y sectores, en particular las cuestiones concretas específicas de uno o varios Estados miembros o de uno o varios sectores.

4. Las revisiones interpares conllevarán visitas *in situ* presenciales o virtuales e intercambios a distancia. En consideración del principio de buena cooperación, los Estados miembros objeto de la revisión facilitarán a los expertos designados la información requerida que sea necesaria para la evaluación de los aspectos examinados. Cualquier información obtenida a través del proceso de revisión interpares se utilizará exclusivamente para tal finalidad. Los expertos que participen en la revisión interpares no divulgarán a terceros ninguna información sensible o confidencial obtenida en el transcurso de dicha revisión.

5. Una vez examinados en un Estado miembro, los mismos aspectos no serán objeto de una revisión interpares ulterior dentro de dicho Estado miembro durante los dos años siguientes a la conclusión de una revisión interpares, a menos que la Comisión decida lo contrario, previa consulta con la ENISA y el Grupo de Cooperación.

6. El Estado miembro velará por que cualquier riesgo de conflicto de intereses que afecte a los expertos designados se comunique a los otros Estados miembros, la Comisión y la ENISA sin demora indebida.

7. Los expertos que participen en revisiones interpares elaborarán informes sobre las constataciones y conclusiones de las revisiones. Los informes se presentarán a la Comisión, el Grupo de Cooperación, la red de CSIRT y la ENISA. Los informes se analizarán en el Grupo de Cooperación y la red de CSIRT. Los informes podrán publicarse en el sitio web específico del Grupo de Cooperación.

CAPÍTULO IV

Obligaciones de gestión de riesgos de ciberseguridad y notificación

SECCIÓN I

Gestión de riesgos de ciberseguridad y notificación

Artículo 17

Gobernanza

1. Los Estados miembros velarán por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 18, supervisen su puesta en práctica y respondan por el incumplimiento de las obligaciones recogidas en el presente artículo por parte de las entidades.

2. Los Estados miembros garantizarán que los miembros del órgano de dirección asistan periódicamente a formaciones específicas para adquirir conocimientos y destrezas suficientes que permitan comprender y evaluar los riesgos de ciberseguridad y las prácticas de gestión y su impacto en las operaciones de la entidad.

Artículo 18

Medidas para la gestión de riesgos de ciberseguridad

1. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan dichas entidades para la prestación de sus servicios. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado.

2. Las medidas a que se hace referencia en el apartado 1 incluirán, al menos, los siguientes elementos:

   a) las políticas de seguridad de los sistemas de información y análisis de riesgos;

   b) la gestión de incidentes (prevención, detección y respuesta a incidentes);

   c) la continuidad de las actividades y la gestión de crisis;

   d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios, como, por ejemplo, proveedores de servicios de almacenamiento y tratamiento de datos o servicios de seguridad administrada;

   e) la seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluida la gestión y divulgación de las vulnerabilidades;

   f) las políticas y los procedimientos (ensayo y auditoría) para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;

g) la utilización de criptografía y cifrado.

3. Los Estados miembros velarán por que, a la hora de estudiar las medidas apropiadas a que se refiere el apartado 2, letra d), las entidades tengan en cuenta las vulnerabilidades específicas de cada proveedor y prestador de servicios y la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

4. Los Estados miembros se asegurarán de que, cuando una entidad constate, respectivamente, que sus servicios o cometidos no se ajustan a los requisitos establecidos en el apartado 2, esta adopte, sin demora indebida, todas las medidas correctoras necesarias para que el servicio en cuestión cumpla dichos requisitos.

5. La Comisión podrá adoptar actos de ejecución para establecer las modalidades técnicas y metodológicas de los elementos a que se refiere el apartado 2. A la hora de elaborar dichos actos, la Comisión procederá con arreglo al procedimiento de examen a que se refiere el artículo 37, apartado 2, y se guiará, en la mayor medida posible, por las normas internacionales y europeas, así como por las especificaciones técnicas pertinentes.

6. La Comisión está facultada para adoptar actos delegados de conformidad con el artículo 36 con objeto de completar los elementos establecidos en el apartado 2 a fin de tener en cuenta nuevas ciberamenazas, la evolución tecnológica o las especificidades sectoriales.

Artículo 19

Evaluaciones coordinadas de la UE de los riesgos de las cadenas de suministro críticas

1. El Grupo de Cooperación, en colaboración con la Comisión y la ENISA, podrán llevar a cabo evaluaciones coordinadas de los riesgos de seguridad de cadenas de suministro de servicios, sistemas o productos de TIC críticos específicos, teniendo en cuenta factores de riesgo técnicos y, cuando proceda, de otra índole.

2. La Comisión, tras consultar al Grupo de Cooperación y a la ENISA, delimitará los servicios, sistemas o productos de TIC críticos específicos que podrán ser objeto de la evaluación coordinada de riesgos a que se refiere el apartado 1.

Artículo 20

Obligaciones de notificación

1. Los Estados miembros velarán por que las entidades esenciales e importantes notifiquen, sin demora indebida, a las autoridades competentes o al CSIRT de conformidad con los apartados 3 y 4 cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. Cuando proceda, dichas entidades notificarán, sin demora indebida, a los destinatarios de sus servicios los incidentes susceptibles de afectar negativamente a la prestación de dicho servicio. Los Estados miembros garantizarán que dichas entidades notifiquen, entre otros detalles,

cualquier información que permita a las autoridades competentes o al CSIRT determinar las repercusiones transfronterizas del incidente.

2. Los Estados miembros se asegurarán de que las entidades esenciales e importantes notifiquen, sin demora indebida, a las autoridades competentes o al CSIRT cualquier ciberamenaza significativa que, a su juicio, podría haber desembocado en un incidente significativo.

Cuando proceda, dichas entidades notificarán, sin demora indebida, a los destinatarios de sus servicios que puedan verse afectados por una ciberamenaza significativa de las medidas o soluciones que dichos destinatarios pueden aplicar en respuesta a la amenaza. Cuando proceda, las entidades notificarán a los destinatarios la propia amenaza. La notificación no sujetará a la entidad notificante a una mayor responsabilidad.

3. Un incidente se considerará significativo si:

a) el incidente ha causado o puede causar perturbaciones operativas o perjuicios económicos sustanciales para la entidad afectada;

b) el incidente ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o morales considerables.

4. Los Estados miembros velarán por que, a los efectos de la notificación con arreglo al apartado 1, las entidades afectadas presenten a las autoridades competentes o al CSIRT:

a) sin demora indebida y en cualquier caso en el plazo de veinticuatro horas desde que se haya tenido constancia del incidente, una notificación inicial en la que se indicará, cuando proceda, si cabe suponer que el incidente responde a una acción ilícita o malintencionada;

b) a instancias de una autoridad competente o un CSIRT, un informe intermedio con las actualizaciones pertinentes sobre la situación;

c) un informe final, a más tardar un mes después de presentar el informe contemplado en la letra a), en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente desencadenó el incidente;

iii) las medidas de mitigación aplicadas y en curso.

Los Estados miembros dispondrán que, en casos debidamente justificados y de acuerdo con las autoridades competentes o el CSIRT, la entidad afectada pueda incumplir los plazos establecidos en las letras a) y c).

5. Las autoridades nacionales competentes o el CSIRT ofrecerá, en el plazo de veinticuatro horas tras la recepción de la notificación inicial a que se refiere el apartado 4, letra a), una respuesta a la entidad notificante, en particular sus comentarios iniciales sobre el incidente y, a instancias de la entidad, una orientación sobre la aplicación de posibles medidas de mitigación. Cuando el CSIRT no haya recibido la notificación a que se refiere el apartado 1, la orientación será proporcionada por la autoridad competente en colaboración con el CSIRT. El CSIRT prestará apoyo técnico adicional cuando así lo solicite la entidad afectada. Cuando se

sospeche que el incidente es de naturaleza delictiva, las autoridades nacionales competentes o el CSIRT también proporcionarán orientación a efectos de denunciar el incidente ante las autoridades policiales.

6. Cuando proceda, y en particular si el incidente mencionado en el apartado 1 afecta a dos o varios Estados miembros, la autoridad competente o el CSIRT al que se haya notificado el incidente informará del mismo a los demás Estados miembros afectados y a la ENISA. Al hacerlo, las autoridades competentes, los CSIRT y los puntos de contacto únicos preservarán, de conformidad con el Derecho de la Unión o de la legislación nacional acorde con el Derecho de la Unión, la seguridad y los intereses comerciales de la entidad, así como la confidencialidad de la información facilitada.

7. Cuando el conocimiento del público sea necesario para evitar un incidente o hacer frente a un incidente en curso, o cuando la divulgación del incidente redunde en el interés público, la autoridad competente o el CSIRT y, en su caso, las autoridades o CSIRT de otros Estados miembros afectados, podrán informar al público, después de consultarlo con la entidad afectada, del incidente o exigir a la entidad que lo haga.

8. A instancias de la autoridad competente o del CSIRT, el punto de contacto único remitirá las notificaciones recibidas de conformidad con los apartados 1 y 2 a los puntos de contacto únicos de otros Estados miembros afectados.

9. El punto de contacto único presentará mensualmente a la ENISA un informe de síntesis que incluya datos anonimizados y agregados sobre los incidentes, los cuasiincidentes y las ciberamenazas significativos notificados con arreglo a los apartados 1 y 2 y al artículo 27. A fin de facilitar el suministro de información comparable, la ENISA podrá publicar orientaciones técnicas sobre los parámetros de la información que debe figurar en el informe de síntesis.

10. Las autoridades competentes facilitarán a las autoridades competentes designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] información sobre los incidentes y las ciberamenazas notificados de conformidad con los apartados 1 y 2 por entidades esenciales identificadas como entidades críticas, o como entidades equivalentes a entidades críticas, conforme a lo dispuesto en dicha Directiva.

11. La Comisión puede adoptar actos de ejecución para especificar en mayor detalle el tipo de información, el formato y el procedimiento de las notificaciones presentadas de conformidad con los apartados 1 y 2. Asimismo, la Comisión podrá adoptar actos de ejecución para precisar los casos en que un incidente se considerará significativo, tal como se contempla en el apartado 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 37, apartado 2.

Artículo 21

Utilización de esquemas europeos de certificación de la ciberseguridad

1. A efectos de demostrar la conformidad con determinados requisitos del artículo 18, los Estados miembros podrán exigir a las entidades esenciales e importantes que certifiquen determinados productos, servicios y procesos de TIC en virtud de un esquema europeo de certificación de la ciberseguridad específico adoptado con arreglo al artículo 49 del Reglamento (UE) 2019/881. Los productos, servicios y

procesos objeto de la certificación podrán ser desarrollados por una entidad esencial o importante o adquiridos a terceros.

2. La Comisión estará facultada para adoptar actos delegados que especifiquen qué categorías de entidades esenciales estarán obligadas a obtener una certificación y en virtud de qué esquemas europeos de certificación de la ciberseguridad específicos conforme al apartado 1. Dichos actos delegados se adoptarán de conformidad con el artículo 36.

3. La Comisión podrá solicitar a la ENISA que prepare una propuesta de esquema de conformidad con el artículo 48, apartado 2, del Reglamento (UE) 2019/881 cuando no haya disponible ningún esquema europeo de certificación de la ciberseguridad apropiado a los efectos del apartado 2.

Artículo 22

Normalización

1. A fin de promover una aplicación convergente de lo dispuesto en el artículo 18, apartados 1 y 2, los Estados miembros fomentarán, sin imponer ni favorecer el uso de un tipo específico de tecnología, la utilización de normas y especificaciones aceptadas a escala europea o internacionalmente que sean pertinentes en materia de seguridad de las redes y los sistemas de información.

2. La ENISA, en colaboración con los Estados miembros, elaborará directrices y orientaciones relativas a las áreas técnicas que deban examinarse en relación con el apartado 1, así como en relación con las normas ya existentes, en particular las normas nacionales de los Estados miembros que permitirían cubrir esas áreas.

Artículo 23

Bases de datos de nombres de dominio y datos de registro

1. A efectos de contribuir a la seguridad, estabilidad y resiliencia del DNS, los Estados miembros velarán por que los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel recopilen y mantengan datos precisos y completos sobre el registro de nombres de dominio en una base de datos con la diligencia debida, respetando la legislación de la Unión en materia de protección de datos por lo que respecta a los datos de carácter personal.

2. Los Estados miembros garantizarán que las bases de datos sobre el registro de nombres de dominio a que se refiere el apartado 1 contengan información pertinente para identificar y contactar con los titulares de los nombres de dominio y los puntos de contacto que administran los nombres de dominio en los dominios de primer nivel.

3. Los Estados miembros se asegurarán de que los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel cuenten con políticas y procedimientos para garantizar que las bases de datos incluyan información precisa y completa. Los Estados miembros velarán por que tales políticas y procedimientos se pongan a disposición del público.

4. Los Estados miembros garantizarán que los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel publiquen, sin demora indebida después del registro de un nombre de dominio, los datos de registro de dominio que no sean de carácter personal.

5. Los Estados miembros se asegurarán de que los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel concedan acceso a datos específicos sobre el registro de nombres de dominio, previa solicitud lícita y debidamente justificada, a los solicitantes de acceso legítimos, de conformidad con la legislación de la Unión en materia de protección de datos. Los Estados miembros velarán por que los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel respondan sin demora indebida a todas las solicitudes de acceso. Los Estados miembros garantizarán que las políticas y los procedimientos de divulgación de dichos datos se pongan a disposición del público.

Sección II

Jurisdicción y registro

Artículo 24

Jurisdicción y territorialidad

1. Los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de redes de distribución de contenidos a que se refiere el anexo I, punto 8, así como los proveedores de servicios digitales a que se refiere el anexo II, punto 6, se considerarán sometidos a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal en la Unión.

2. A los efectos de la presente Directiva, se considerará que el establecimiento principal en la Unión de las entidades a que se refiere el apartado 1 se encuentra en el Estado miembro en el que se adopten las decisiones relativas a las medidas para la gestión de riesgos de ciberseguridad. En caso de que dichas decisiones no se adopten en un establecimiento dentro de la Unión, se considerará que el establecimiento principal se encuentra en el Estado miembro en el que las entidades tienen el establecimiento con mayor número de trabajadores en la Unión.

3. Si una entidad contemplada en el apartado 1 no está establecida en la Unión, pero ofrece servicios dentro de esta, designará un representante en ella. El representante se establecerá en uno de aquellos Estados miembros en los que se ofrecen los servicios. Dicha entidad se considerará sometida a la jurisdicción del Estado miembro en el que se encuentre establecido su representante. En ausencia de un representante designado dentro de la Unión con arreglo al presente artículo, cualquier Estado miembro en el que la entidad preste servicios podrá emprender acciones legales contra la entidad por incumplimiento de las obligaciones recogidas en la presente Directiva.

4. La designación de un representante por una entidad contemplada en el apartado 1 se entenderá sin perjuicio de las acciones legales que pudieran emprenderse contra la propia entidad.

Artículo 25

Registro de entidades esenciales e importantes

1. La ENISA creará y mantendrá un registro de entidades esenciales e importantes a que se refiere el artículo 24, apartado 1. Las entidades remitirán la siguiente información a la ENISA a más tardar [doce meses después de la entrada en vigor de la Directiva]:

   a) el nombre de la entidad;

   b) la dirección de su establecimiento principal y del resto de sus establecimientos legales en la Unión o, de no estar establecida en la Unión, de su representante designado en virtud del artículo 24, apartado 3;

   c) los datos de contacto actualizados, en particular las direcciones de correo electrónico y los números de teléfono de las entidades.

2. Las entidades a que se refiere el apartado 1 notificarán a la ENISA cualquier cambio en la información remitida con arreglo al apartado 1 sin demora, y en cualquier caso, en el plazo de tres meses desde la fecha en que se produjo el cambio.

3. Tras la recepción de la información contemplada en el apartado 1, la ENISA la transmitirá a los puntos de contacto únicos en función de la ubicación del establecimiento principal de cada entidad que se ha indicado o, si no está establecida en la Unión, de su representante designado. Cuando, además de con su establecimiento principal en la Unión, una entidad a que se refiere el apartado 1 cuente con establecimientos adicionales en otros Estados miembros, la ENISA también informará a los puntos de contacto únicos de dichos Estados miembros.

4. En caso de que una entidad no registre su actividad o no facilite la información pertinente dentro del plazo fijado en el apartado 1, cualquier Estado miembro en el que la entidad preste servicios será competente para garantizar que dicha entidad cumpla las obligaciones establecidas en la presente Directiva.

CAPÍTULO V

Intercambio de información

Artículo 26

Mecanismos de intercambio de información sobre ciberseguridad

1. Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, los Estados miembros velarán por que las entidades esenciales e importantes puedan intercambiar entre sí información sobre ciberseguridad pertinente, en particular la referente a ciberamenazas, vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, siempre que dicho intercambio de información:

   a) se haga con el objetivo de prevenir, detectar, responder o mitigar incidentes;

   b) refuerce el nivel de ciberseguridad, en particular al concienciar sobre las ciberamenazas, limitar o impedir la capacidad de tales amenazas para

propagarse, o respaldar una batería de capacidades de defensa, corrección y divulgación de las vulnerabilidades, técnicas de detección de amenazas, estrategias de mitigación o etapas de respuesta y recuperación.

2. Los Estados miembros garantizarán que el intercambio de información se desarrolle dentro de comunidades de confianza de entidades esenciales e importantes. Dicho intercambio se pondrá en práctica a través de mecanismos de intercambio de información que respeten la posible naturaleza delicada de la información compartida y de conformidad con las normas de la legislación de la Unión a que se refiere el apartado 1.

3. Los Estados miembros establecerán normas que precisen el procedimiento, los elementos operativos (incluido el uso de plataformas de TIC específicas), el contenido y las condiciones de los mecanismos de intercambio de información a que se refiere el apartado 2. Asimismo, dichas normas establecerán los detalles de la participación de las autoridades públicas en los mecanismos mencionados, así como los elementos operativos, incluido el uso de plataformas de TIC específicas. Los Estados miembros prestarán apoyo a la aplicación de dichos mecanismos de conformidad con las correspondientes políticas a que se refiere el artículo 5, apartado 2, letra g).

4. Las entidades esenciales e importantes notificarán a las autoridades competentes su participación en los mecanismos de intercambio de información a que se refiere el apartado 2 cuando se incorporen a dichos mecanismos o, cuando proceda, su retirada de dichos mecanismos cuando la retirada surta efecto.

5. De conformidad con el Derecho de la Unión, la ENISA prestará su apoyo al establecimiento de mecanismos de intercambio de información sobre ciberseguridad a que se refiere el apartado 2 mediante el suministro de buenas prácticas y orientación.

Artículo 27

Notificación voluntaria de información pertinente

Los Estados miembros velarán por que, sin perjuicio de lo dispuesto en el artículo 3, las entidades excluidas del ámbito de aplicación de la presente Directiva puedan presentar voluntariamente notificaciones de ciberamenazas, cuasiincidentes e incidentes significativos. Cuando tramiten las notificaciones, los Estados miembros actuarán de conformidad con el procedimiento establecido en el artículo 20. Los Estados miembros podrán dar prioridad a la tramitación de notificaciones obligatorias sobre las notificaciones voluntarias. La notificación voluntaria no dará lugar a la imposición de obligaciones adicionales a la entidad notificante a las que no estaría sujeta de no haber presentado dicha notificación.

CAPITULO VI

Supervisión y ejecución

Artículo 28

Aspectos generales relativos a la supervisión y la ejecución

1. Los Estados miembros velarán por que las autoridades competentes supervisen efectivamente y adopten las medidas necesarias para garantizar el cumplimiento de la presente Directiva, en particular las obligaciones establecidas en los artículos 18 y 20.

2. Las autoridades competentes cooperarán estrechamente con las autoridades responsables de la protección de datos a la hora de hacer frente a incidentes que den lugar a violaciones de la seguridad de los datos personales.

Artículo 29

Supervisión y ejecución en el caso de entidades esenciales

1. Los Estados miembros garantizarán que las medidas de supervisión o ejecución impuestas a las entidades esenciales en relación con las obligaciones contempladas en la presente Directiva sean efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual.

2. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus funciones de supervisión en relación con entidades esenciales, dispongan de competencias para someter a dichas entidades a:

   a) inspecciones *in situ* y supervisión a distancia, incluidos controles aleatorios;

   b) auditorías periódicas;

   c) auditorías de seguridad específicas basadas en evaluaciones de riesgos o en información disponible sobre los riesgos;

   d) análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes;

   e) solicitudes de información necesaria para evaluar las medidas de ciberseguridad adoptadas por la entidad, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de notificar a la ENISA con arreglo al artículo 25, apartados 1 y 2;

   f) solicitudes de acceso a datos, documentos o cualquier información necesaria para el desempeño de sus funciones de supervisión;

   g) solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.

3. En el ejercicio de sus competencias con arreglo al apartado 2, letras e) a g), las autoridades competentes indicarán la finalidad de la solicitud y especificarán la información requerida.

4. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus facultades de ejecución en relación con entidades esenciales, dispongan de competencias para:

   (a) apercibir a las entidades por el incumplimiento de las obligaciones establecidas en la presente Directiva;

(b) emitir instrucciones vinculantes o una orden de requerimiento para que dichas entidades subsanen las deficiencias detectadas o las infracciones de las obligaciones establecidas en la presente Directiva;

(c) exigir a dichas entidades que pongan fin a las conductas que incumplan las obligaciones establecidas en la presente Directiva y que se abstengan de repetirlas;

(d) exigir a dichas entidades que adecúen sus medidas de gestión de riesgos u obligaciones de notificación a las obligaciones establecidas en los artículos 18 y 20 de una manera específica y en un plazo concreto;

(e) ordenar a dichas entidades que informen a las personas físicas o jurídicas a las que prestan servicios o actividades que puedan verse afectadas por una ciberamenaza significativa de cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza;

(f) ordenar a dichas entidades que apliquen las recomendaciones formuladas a raíz de una auditoría de seguridad en un plazo razonable;

(g) designar un responsable de supervisión con tareas claramente definidas para que supervise, a lo largo de un período determinado, el cumplimiento de sus obligaciones previstas en los artículos 18 y 20;

(h) ordenar a dichas entidades que hagan públicos aspectos del incumplimiento de las obligaciones establecidas en la presente Directiva de una manera específica;

(i) emitir un comunicado público en el que se identifique a las personas físicas y jurídicas responsables del incumplimiento de una obligación establecida en la presente Directiva y la naturaleza de tal incumplimiento;

(j) imponer o solicitar la imposición por parte de los organismos o los órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 31 a título adicional o sustitutivo de las medidas referidas en las letras a) a i) del presente apartado, en función de las circunstancias de cada caso particular.

5. Cuando las medidas de ejecución adoptadas con arreglo al apartado 4, letras a) a d) y f), resulten ineficaces, los Estados miembros garantizarán que las autoridades competentes estén facultadas para fijar un plazo en el que se requerirá a la entidad esencial que adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de dichas autoridades. Si las medidas requeridas no se adoptan dentro del plazo establecido, los Estados miembros velarán por que las autoridades competentes estén facultadas para:

a) suspender o solicitar a un organismo de certificación o autorización que suspenda una certificación o autorización referente a una parte o la totalidad de los servicios o actividades prestados por una entidad esencial;

b) imponer o solicitar la imposición por parte de los organismos o los órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una prohibición temporal sobre cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial, y de cualquier otra persona física responsable del incumplimiento, de ejercer funciones de dirección en dicha entidad.

Las sanciones referidas se aplicarán únicamente hasta que la entidad adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente a instancias de la cual se aplicaron las sanciones.

6. Los Estados miembros garantizarán que cualquier persona física responsable de una entidad esencial o que actúe como representante de ella con facultades para representarla, la autoridad para tomar decisiones en su nombre o la autoridad para ejercer control sobre ella tenga competencias para velar por que cumpla las obligaciones establecidas en la presente Directiva. Los Estados miembros velarán por que dichas personas físicas puedan considerarse responsables por el incumplimiento de su deber de garantizar el cumplimiento de las obligaciones establecidas en la presente Directiva.

7. Cuando se adopte una medida de ejecución o se aplique una sanción con arreglo a los apartados 4 y 5, las autoridades competentes observarán el derecho de defensa y tendrán en cuenta las circunstancias de cada caso particular, como mínimo los siguientes aspectos:

   a) la gravedad del incumplimiento y la importancia de las disposiciones infringidas. Entre las infracciones que deben considerarse graves cabe destacar los incumplimientos reiterados, la ausencia de notificación o subsanación de los incidentes con un efecto perturbador significativo, la ausencia de subsanación de deficiencias tras recibir instrucciones vinculantes de las autoridades competentes, la obstrucción de las actividades de fiscalización o control ordenadas por la autoridad competente tras la constatación de una infracción, el suministro de información falsa o manifiestamente imprecisa en relación con los requisitos de gestión del riesgo o las obligaciones de notificación previstos en los artículos 18 y 20.

   b) la duración del incumplimiento, en particular si ha habido incumplimientos reiterados;

   c) los perjuicios o las pérdidas reales originados, o los perjuicios o las pérdidas que podrían haberse originado, en la medida en que puedan determinarse. A la hora de evaluar este aspecto, se tendrán en cuenta, entre otros factores, las pérdidas financieras o económicas reales o potenciales, los efectos para otros servicios y el número de usuarios afectados o potencialmente afectados;

   d) la intencionalidad o negligencia en la infracción;

   e) las medidas adoptadas por la entidad para prevenir o reducir los perjuicios o las pérdidas;

   f) la adhesión a códigos de conducta o a mecanismos de certificación aprobados;

   g) el grado de cooperación de las personas físicas o jurídicas responsables con las autoridades competentes.

8. Las autoridades competentes argumentarán detalladamente sus decisiones de ejecución. Antes de tomar dichas decisiones, las autoridades competentes notificarán a las entidades afectadas sus constataciones preliminares y concederán a dichas entidades un plazo razonable para formular observaciones.

9. Los Estados miembros velarán por que sus autoridades competentes informen a las autoridades competentes del Estado miembro afectado designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] cuando ejerzan sus facultades de supervisión y ejecución con objeto de

garantizar el cumplimiento por parte de una entidad esencial identificada como crítica, o como una entidad equivalente a una entidad crítica, con arreglo a dicha Directiva, de las obligaciones conforme a la presente Directiva. A instancias de las autoridades competentes en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas], las autoridades competentes podrán ejercer sus facultades de supervisión y ejecución respecto a una entidad esencial identificada como crítica o equivalente.

Artículo 30

Supervisión y ejecución en el caso de entidades importantes

1. Cuando dispongan de pruebas o indicios de que una entidad importante no cumple las obligaciones establecidas en la presente Directiva, y en particular en los artículos 18 y 20, los Estados miembros garantizarán que las autoridades competentes actúen, cuando proceda, a través de medidas de supervisión *a posteriori*.

2. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus tareas de supervisión en relación con entidades importantes, dispongan de competencias para someter a dichas entidades a:

   a) inspecciones *in situ* y supervisión *a posteriori* a distancia;

   b) auditorías de seguridad específicas basadas en evaluaciones de riesgos o en información disponible sobre los riesgos;

   c) análisis de seguridad basados en criterios de evaluación del riesgo objetivos, justos y transparentes;

   d) solicitudes de toda información necesaria para evaluar *a posteriori* las medidas de ciberseguridad, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de notificar a la ENISA con arreglo al artículo 25, apartados 1 y 2;

   e) solicitudes de acceso a datos, documentos o cualquier información necesaria para el desempeño de las funciones de supervisión.

3. En el ejercicio de sus competencias con arreglo al apartado 2, letras d) o g), las autoridades competentes indicarán la finalidad de la solicitud y especificarán la información requerida.

4. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus facultades de ejecución en relación con entidades importantes, dispongan de competencias para:

   a) apercibir a las entidades por el incumplimiento de las obligaciones establecidas en la presente Directiva;

   b) emitir instrucciones vinculantes o una orden de requerimiento para que dichas entidades subsanen las deficiencias detectadas o la infracción de las obligaciones establecidas en la presente Directiva;

   c) exigir a dichas entidades que pongan fin a las conductas que incumplan las obligaciones establecidas en la presente Directiva y que se abstengan de repetirlas;

d) exigir a dichas entidades que adecúen sus medidas de gestión de riesgos u obligaciones de notificación a las obligaciones establecidas en los artículos 18 y 20 de una manera específica y en un plazo concreto;

e) ordenar a dichas entidades que informen a las personas físicas o jurídicas a las que prestan servicios o actividades que puedan verse afectadas por una ciberamenaza significativa de cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza;

f) ordenar a dichas entidades que apliquen las recomendaciones formuladas a raíz de una auditoría de seguridad en un plazo razonable;

g) ordenar a dichas entidades que hagan públicos aspectos del incumplimiento de sus obligaciones establecidas en la presente Directiva de una manera específica;

h) emitir un comunicado público en el que se identifique a las personas físicas y jurídicas responsables del incumplimiento de una obligación establecida en la presente Directiva y la naturaleza de tal incumplimiento;

i) imponer o solicitar la imposición por parte de los órganos o tribunales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 31 a título adicional o sustitutivo de las medidas referidas en las letras a) a h) del presente apartado, en función de las circunstancias de cada caso particular.

5. El artículo 29, apartados 6 a 8, se aplicará asimismo a las medidas de supervisión y ejecución previstas en el presente artículo en el caso de las entidades importantes enumeradas en el anexo II.

Artículo 31

Condiciones generales para la imposición de multas administrativas a entidades esenciales e importantes

1. Los Estados miembros velarán por que las multas administrativas impuestas a entidades esenciales e importantes al amparo del presente artículo en relación con el incumplimiento de las obligaciones establecidas en la presente Directiva sean, en cada caso particular, efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 29, apartado 4, letras a) a i), el artículo 29, apartado 5, y el artículo 30, apartado 4, letras a) a h).

3. A la hora de decidir la imposición de una multa administrativa y su cuantía en cada caso particular se tendrán debidamente en cuenta, como mínimo, los elementos contemplados en el artículo 29, apartado 7.

4. Los Estados miembros garantizarán que el incumplimiento de las obligaciones establecidas en los artículos 18 o 20 se sancione, de acuerdo con los apartados 2 y 3 del presente artículo, con multas administrativas de al menos 10 000 000 EUR o de una cuantía equivalente como máximo al 2 % del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad esencial durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

5. Los Estados miembros pueden prever la facultad de imponer multas coercitivas para obligar a una entidad esencial o importante a poner fin a una infracción de conformidad con una decisión previa de la autoridad competente.

6. Sin perjuicio de las facultades de las autoridades competentes conferidas en virtud de los artículos 29 y 30, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a las entidades de la Administración pública a que se refiere el artículo 4, punto 23, sujetas a las obligaciones previstas en la presente Directiva.

Artículo 32

Infracciones que conllevan una violación de la seguridad de los datos personales

1. Cuando las autoridades competentes tengan indicios de que el incumplimiento de las obligaciones establecidas en los artículos 18 y 20 cometido por una entidad esencial o importante conlleva una violación de la seguridad de los datos personales en el sentido del artículo 4, punto 12, del Reglamento (UE) 2016/679 que deba notificarse en virtud del artículo 33 de este, informarán a las autoridades de control competentes en virtud de los artículos 55 y 56 de dicho Reglamento en un plazo de tiempo razonable.

2. Cuando las autoridades de control competentes de conformidad con los artículos 55 y 56 del Reglamento (UE) 2016/679 decidan ejercer sus facultades con arreglo al artículo 58, apartado 2, letra i), de dicho Reglamento e imponer una multa administrativa, las autoridades competentes no impondrán una multa administrativa por la misma infracción en virtud del artículo 31 de la presente Directiva. No obstante lo dispuesto, las autoridades competentes podrán aplicar las medidas de ejecución o ejercer las facultades sancionadoras previstas en el artículo 29, apartado 4, letras a) a i), el artículo 29, apartado 5, y el artículo 30, apartado 4, letras a) a h), de la presente Directiva.

3. Cuando la autoridad de control competente en virtud del Reglamento (UE) 2016/679 esté establecida en un Estado miembro distinto al de la autoridad competente, la autoridad competente podrá informar a la autoridad de control establecida en el mismo Estado miembro.

Artículo 33

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. Tales sanciones serán efectivas, proporcionadas y disuasorias.

2. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, a más tardar [dos] años después de la entrada en vigor de la presente Directiva, y le notificarán sin demora indebida cualquier modificación posterior.

Artículo 34

Asistencia mutua

1. Cuando una entidad esencial o importante preste servicios en más de un Estado miembro o tenga su establecimiento principal o un representante en un Estado miembro, pero sus redes y sistemas de información en otro u otros Estados miembros, la autoridad competente del Estado miembro en el que se encuentre su establecimiento principal, otro establecimiento o el representante y las autoridades competentes de esos otros Estados miembros cooperarán entre sí y se asistirán mutuamente cuando sea necesario. Dicha cooperación implicará, como mínimo, lo siguiente:

   a) que las autoridades competentes que apliquen medidas de supervisión o ejecución en un Estado miembro informen y consulten a través del punto de contacto único a las autoridades competentes de los otros Estados miembros afectados sobre las medidas de supervisión y ejecución adoptadas y su seguimiento, de conformidad con los artículos 29 y 30;

   b) que una autoridad competente pueda solicitar a otra autoridad competente que adopte las medidas de supervisión o ejecución a que se refieren los artículos 29 y 30;

   c) que una autoridad competente, al recibir una solicitud justificada de otra autoridad competente, preste a la otra autoridad competente asistencia para que las medidas de supervisión o ejecución a que se refieren los artículos 29 y 30 puedan aplicarse de manera efectiva, eficiente y coherente. Dicha asistencia mutua podrá abarcar solicitudes de información y medidas de supervisión, incluidas las solicitudes para la realización de inspecciones *in situ*, supervisión a distancia o auditorías de seguridad específicas. La autoridad competente destinataria de una solicitud de asistencia no podrá negarse a ella a menos que, tras dialogar con las otras autoridades interesadas, la ENISA y la Comisión, se determine que o bien la autoridad carece de competencias para prestar la asistencia requerida, o bien dicha asistencia no se adecúa a las tareas de supervisión de la autoridad competente desempeñadas de conformidad con los artículos 29 o 30.

2. Cuando proceda y de común acuerdo, las autoridades competentes de Estados miembros diferentes podrán emprender las medidas conjuntas de supervisión a que se refieren los artículos 29 y 30.

CAPÍTULO VII

Disposiciones transitorias y finales

Artículo 35

Revisión

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. En concreto, el informe evaluará la importancia de los sectores, los subsectores, el tamaño y el tipo de las entidades a que se refieren los anexos I y II para el funcionamiento de la economía y la sociedad por lo que respecta a la ciberseguridad.

A tal efecto y con vistas a ampliar la cooperación estratégica y operativa, la Comisión tendrá en cuenta los informes del Grupo de Cooperación y de la red de CSIRT sobre la experiencia adquirida a nivel estratégico y operativo. El primer informe se presentará a más tardar el… [cincuenta y cuatro meses después de la fecha de entrada en vigor de la presente Directiva].

Artículo 36

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, apartado 6, y en el artículo 21, apartado 2, se otorgan a la Comisión por un período de cinco años a partir del […]
3. La delegación de poderes mencionada en el artículo 18, apartado 6, y en el artículo 21, apartado 2, 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, apartado 6, y del artículo 21, apartado 2, 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 37

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.
3. Cuando el dictamen del comité deba obtenerse mediante procedimiento escrito, se pondrá fin a dicho procedimiento sin resultado si, en el plazo para la emisión del dictamen, el presidente del comité así lo decide o si un miembro del comité así lo solicita.

Artículo 38

Transposición

1. Los Estados miembros adoptarán y publicarán a más tardar el … [dieciocho meses después de la fecha de entrada en vigor de la presente Directiva] las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del … [un día después de la fecha mencionada en el párrafo primero].

2. 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.

Artículo 39

Modificación del Reglamento (UE) n.º 910/2014

Se suprime el artículo 19 del Reglamento (UE) n.º 910/2014.

Artículo 40

Modificación de la Directiva (UE) 2018/1972

Se suprimen los artículos 40 y 41 de la Directiva (UE) 2018/1972.

Artículo 41

Derogación

Queda derogada la Directiva (UE) 2016/1148 con efectos a partir del.. [fecha del plazo de transposición de la Directiva].

Las referencias a la Directiva (UE) 2016/1148 se entenderán hechas a la presente Directiva y se leerán con arreglo a la tabla de correspondencias que figura en el anexo III.

Artículo 42

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 43

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Bruselas, el

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

FICHA FINANCIERA LEGISLATIVA

Índice

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

1.2. Ámbito(s) político(s) afectado(s) *(Clúster de programas)*

Redes de Comunicación, Contenido y Tecnologías

1.3. La propuesta/iniciativa se refiere a:

☐ **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto/una acción preparatoria**[40]

☒ **la prolongación de una acción existente**

☐ **una fusión o reorientación de una o más acciones hacia otra/una nueva acción**

1.4. Justificación de la propuesta/iniciativa

1.4.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado para la aplicación de la iniciativa

El objetivo de la revisión es incrementar el nivel de ciberresiliencia de un conjunto exhaustivo de empresas que operan en la Unión Europea en todos los sectores pertinentes, reducir las incoherencias en términos de resiliencia en todo el mercado interior en los sectores que ya están cubiertos por la Directiva y mejorar el nivel de conciencia situacional conjunta y la capacidad colectiva de preparación y respuesta.

1.4.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como una mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, por «valor añadido de la intervención de la Unión» se entenderá el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

La resiliencia en términos de ciberseguridad en toda la Unión no puede ser eficaz si se aplican distintos enfoques de carácter nacional o regional. La Directiva SRI solucionó esta deficiencia al establecer un marco para la seguridad de las redes y los sistemas de información a escala nacional y de la Unión. No obstante, la primera revisión periódica de la Directiva SRI señaló una serie de fallos inherentes que, en última instancia, han culminado en disparidades considerables entre los Estados miembros en términos de capacidades, planificación y nivel de protección que afectan al mismo tiempo a las condiciones de competencia equitativas para empresas similares en el mercado interior. Los siguientes motivos justifican que la intervención de la UE trascienda las medidas actuales de la Directiva SRI: i) la naturaleza transfronteriza del problema; ii) el potencial de que la intervención de la UE mejore unas políticas nacionales efectivas y las facilite; y iii) la contribución de unas acciones políticas concertadas y colaborativas a la protección efectiva de los datos y la privacidad.

[40] Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero.

De esta manera, los objetivos indicados pueden alcanzarse mejor a través de la actuación de la Unión que por los Estados miembros en solitario.

1.4.3. Principales conclusiones extraídas de experiencias similares anteriores

La Directiva SRI es el primer instrumento horizontal del mercado interior destinado a mejorar la resiliencia de las redes y los sistemas en la Unión frente a los riesgos de ciberseguridad. Asimismo, ha contribuido en gran medida a aumentar el nivel común de ciberseguridad entre los Estados miembros. No obstante, la revisión del funcionamiento y la aplicación de la Directiva han puesto de manifiesto varias deficiencias que, además del aumento de la digitalización y la necesidad de una respuesta más actualizada, deben subsanarse en un acto jurídico revisado.

1.4.4. Compatibilidad y posibles sinergias con otros instrumentos adecuados

La nueva propuesta es plenamente coherente y consecuente con otras iniciativas relacionadas, como la propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero y la propuesta de Directiva sobre la resiliencia de los operadores críticos de servicios esenciales. Asimismo, es coherente con el Código Europeo de las Comunicaciones Electrónicas, el Reglamento General de Protección de Datos y el Reglamento eIDAS.

La propuesta es un componente fundamental de la Estrategia de la UE para una Unión de la Seguridad.

1.5. Duración e incidencia financiera

☐ **duración limitada**

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

– ☐ Incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.

☒ **duración ilimitada**

– Ejecución: fase de puesta en marcha desde 2022 hasta 2025

– y pleno funcionamiento a partir de la última fecha.

1.6. Modo(s) de gestión previsto(s)[41]

Gestión directa a cargo de la Comisión

– ☒ por sus servicios, incluido su personal en las delegaciones de la Unión;

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

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

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especifíquense);

– ☐ el Banco Europeo de Inversiones (BEI) y el Fondo Europeo de Inversiones;

– X☐ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

– ☐ organismos de Derecho público;

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

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

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

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

Observaciones

La Agencia de la Unión Europea para la Ciberseguridad (ENISA), a la que se ha otorgado un nuevo mandato permanente a través del Reglamento sobre la Ciberseguridad, prestaría asistencia a los Estados miembros y a la Comisión en la aplicación de la Directiva SRI revisada.

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

Como resultado de la Directiva SRI revisada, a partir del año 2022/2023, la ENISA tendrá ámbitos de actuación adicionales. Aunque estos ámbitos de actuación estarían cubiertos por las funciones generales de la ENISA de acuerdo con su mandato, se traducirán en un aumento de la carga de trabajo para la Agencia. Más concretamente, aparte de sus ámbitos de actuación actuales, en virtud de la propuesta de la Comisión de Directiva SRI revisada la ENISA deberá también incorporar específicamente a su programa de trabajo las siguientes funciones a título ilustrativo: i) desarrollar y mantener un Registro Europeo de Vulnerabilidades (artículo 6, apartado 2, de la propuesta), ii) hacerse cargo de la secretaría de la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) (artículo 14 de la propuesta) y publicar un informe anual sobre la situación de la ciberseguridad en la UE (artículo 15 de la propuesta), iii) prestar apoyo a la organización de revisiones interpares entre los Estados miembros (artículo 16 de la propuesta), iv) recopilar datos agregados sobre incidentes de los Estados miembros y publicar orientaciones técnicas (artículo 20, apartado 9, de la propuesta), y v) crear y mantener un registro de entidades que presten servicios transfronterizos (artículo 25 de la propuesta).

Por consiguiente, se solicitarán cinco ETC adicionales a partir de 2022 con un presupuesto para cubrir estos nuevos puestos que asciende a aproximadamente a 0,61 millones EUR al año (véase la ficha financiera separada para las agencias).

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

La Comisión revisará periódicamente el funcionamiento de la Directiva e informará al Parlamento Europeo y al Consejo, por primera vez tres años después de la entrada en vigor.

Asimismo, la Comisión evaluará la correcta transposición de la Directiva por parte de los Estados miembros.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

La unidad de la DG CNECT responsable del ámbito político gestionará la aplicación de la Directiva.

2.2.2. Información relativa a los riesgos identificados y al sistema o los sistemas de control interno establecidos para mitigarlos

Riesgo muy bajo, puesto que el ecosistema de la Directiva SRI ya está instaurado.

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados») y evaluación del nivel de riesgo de error previsto (al pago y al cierre)

No procede. Uso exclusivo del presupuesto administrativo («dotación global»).

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

No procede. Uso exclusivo del presupuesto administrativo («dotación global»).

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

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

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número [Rúbrica…7……...……]	CD/CND[42]	de países de la AELC[43]	de países candidatos[44]	de terceros países	a efectos de lo dispuesto en el artículo [21, apartado 2, letra b)], del Reglamento Financiero
	20 02 06 gastos de gestión 20 02 06	CND	NO	NO	NO	NO

[42] CD = créditos disociados / CND = créditos no disociados.

[43] AELC: Asociación Europea de Libre Comercio.

[44] Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	**<…>**	[Rúbrica……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Después de 2027***	**TOTAL**
Créditos de operaciones (desglosados conforme a las líneas presupuestarias que figuran en el punto 3.1)	Compromisos	(1)									
	Pagos	(2)									
Créditos de carácter administrativo financiados mediante la dotación del programa[45]	Compromisos = Pagos	(3)									
TOTAL de los créditos de la dotación del programa	Compromisos	=1+3									
	Pagos	=2+3									

Rúbrica del marco financiero plurianual	7	«Gastos administrativos» Reuniones: las reuniones plenarias del Grupo de Cooperación SRI se suelen celebrar cuatro veces al año. La Comisión sufraga los gastos asociados al *catering* y los gastos de desplazamiento de representantes de veintisiete Estados miembros (un representante por cada uno de ellos). Los costes de una reunión pueden alcanzar los 15 000 EUR. Misiones: las misiones están relacionadas con el seguimiento de la aplicación de la Directiva SRI. Ejemplo: En un año (mayo de 2019 a julio de 2020), estaba previsto

[45] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

		organizar las denominadas visitas en el contexto de la SRI y visitar a los veintisiete Estados miembros para analizar la aplicación de la Directiva SRI en toda la UE.

Esta sección debe rellenarse mediante «los datos presupuestarios de carácter administrativo» que deben introducirse primero en el anexo de la ficha financiera legislativa, que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		2021	2022	2023	2024	2025	2026	2027	*Después de 2027*	TOTAL
Recursos humanos		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Otros gastos administrativos		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
TOTAL de los créditos de la RÚBRICA 7 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

En millones EUR (al tercer decimal)

		2021	2022	2023	2024	2025	2026	2027	*Después de 2027*	TOTAL
TOTAL de los créditos de las distintas RÚBRICAS del marco financiero plurianual	Compromisos									
	Pagos									

3.2.2. Resumen de la incidencia estimada en los créditos de carácter administrativo

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

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

En millones EUR (al tercer decimal)

Años	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
RÚBRICA 7 del marco financiero plurianual								
Recursos humanos	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Otros gastos administrativos	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Subtotal para la RÚBRICA 7 del marco financiero plurianual	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Al margen de la RÚBRICA 7[46] of the multiannual financial framework								
Recursos humanos								
Otros gastos de carácter administrativo								
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual								

TOTAL	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción y/o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

[46] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.2.1. Necesidades estimadas de recursos humanos

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

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

Estimación que debe expresarse en unidades de equivalente a jornada completa

Años		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Empleos de plantilla (funcionarios y personal temporal)								
Sede y Oficinas de Representación de la Comisión		6	6	6	6	6	6	6
Delegaciones								
Investigación								
• Personal externo (en unidades de equivalente a tiempo completo: ETC): AC, AL, ENCS, INT y JED[47] Rúbrica 7								
Financiado con cargo a la RÚBRICA 7 del marco financiero plurianual	- en la sede	3	3	3	3	3	3	3
	- en las Delegaciones							
Financiado con cargo a la dotación del programa [48]	- en la sede							
	- en las Delegaciones							
Investigación								
Otro (especifíquese)								
TOTAL		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	• Elaboración de actos delegados de conformidad con el artículo 18, apartado 6, el artículo 21, apartado 2, y el artículo 36. • Elaboración de actos de ejecución de conformidad con el artículo 12, apartado 8, el artículo 18, apartado 5, y el artículo 20, apartado 11. • Proporcionar una secretaría para el Grupo de Cooperación SRI. • Organización de las reuniones plenarias y las reuniones de las líneas de trabajo del Grupo de Cooperación SRI. • Coordinación del trabajo de los Estados miembros en diversos documentos (directrices, herramientas, etc.). • Ejercer de enlace con otros servicios de la Comisión, la ENISA y las autoridades nacionales con vistas a la aplicación de la Directiva SRI. • Análisis de buenas prácticas y métodos nacionales relacionados con la aplicación de la Directiva SRI.
Personal externo	Apoyo a todas las funciones anteriores según proceda

47 AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD= joven profesional en delegación.

48 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

3.2.3. Contribución de terceros

La propuesta/iniciativa:

– X☐ no prevé la cofinanciación por terceros

– ☐ prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

Años	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

3.3. Incidencia estimada en los ingresos

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

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

☐ en los recursos propios

☐ en otros ingresos

indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Incidencia de la propuesta/iniciativa[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artículo ….							

En el caso de los ingresos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

Otras observaciones (por ejemplo, método/fórmula que se utiliza para calcular la incidencia en los ingresos o cualquier otra información).

[49] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos una vez deducido el 20 % de los gastos de recaudación.

ANEXO
de la FICHA FINANCIERA LEGISLATIVA

Nombre de la propuesta/iniciativa:

Propuesta de Directiva por la que se revisa la 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

……
……

1. NÚMERO y COSTE de los RECURSOS HUMANOS QUE SE CONSIDERAN NECESARIOS

2. COSTE de OTROS GASTOS ADMINISTRATIVOS

3. MÉTODOS de CÁLCULO UTILIZADOS para ESTIMAR LOS COSTES

3.1 Recursos humanos

3.2 Otros gastos administrativos

*El presente anexo, **que debe cumplimentar cada DG/servicio que participe en la propuesta/iniciativa**, debe acompañar a la ficha financiera legislativa cuando se ponga en marcha la consulta entre servicios.*

Los cuadros de datos se utilizan como fuente de cara a los cuadros que figuran en la ficha financiera legislativa. Son de uso estrictamente interno dentro de la Comisión.

1. Coste de los recursos humanos que se consideran necesarios

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

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

En millones EUR (al tercer decimal)

RÚBRICA 7 del marco financiero plurianual		2021		2022		2023		2024		2025		2026		2027		TOTAL	
		ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos
• Empleos de plantilla (funcionarios y personal temporal)																	
Sede y Oficinas de Representación de la Comisión	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
en Delegaciones de la Unión	AD																
	AST																
• Personal externo [50]		0,24															
Dotación global	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	ENCS																
	INT																
en Delegaciones de la Unión	AC																
	AL																

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

	ENCS																
	INT																
	JPD																
Otras líneas presupuestarias (*especifíquense*)																	
Subtotal para la RÚBRICA 7 del marco financiero plurianual		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Al margen de la RÚBRICA 7 del marco financiero plurianual		2021		2022		2023		2024		2025		2025		2025		TOTAL	
		ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos	ETC	Créditos
• Empleos de plantilla (funcionarios y personal temporal)																	
Investigación	AD																
	AST																
• Personal externo [51]																	
Personal externo con cargo a créditos operativos (antiguas líneas «BA»).	- en la sede	AC															
		ENCS															
		INT															
	- en Delegaciones de la Unión	AC															
		AL															
		ENCS															
		INT															
		JPD															
Investigación)		AC															
		ENCS															
		INT															

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

Otras líneas presupuestarias (*especifíquense*)																	
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual																	

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Incidencia estimada en los recursos humanos de la ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA), a la que se ha otorgado un nuevo mandato permanente a través del Reglamento sobre la Ciberseguridad, prestaría asistencia a los Estados miembros y a la Comisión en la aplicación de la Directiva SRI revisada.

Como resultado de la Directiva SRI revisada, a partir del año 2022/2023, la ENISA tendrá ámbitos de actuación adicionales. Aunque estos ámbitos de actuación estarían cubiertos por las funciones generales de la ENISA de acuerdo con su mandato, se traducirán en un aumento de la carga de trabajo para la Agencia. Más concretamente, aparte de sus ámbitos de actuación actuales, en virtud de la propuesta de la Comisión de Directiva SRI revisada la ENISA deberá también incorporar específicamente a su programa de trabajo las siguientes funciones a título ilustrativo: i) desarrollar y mantener un Registro Europeo de Vulnerabilidades (artículo 6, apartado 2, de la propuesta), ii) hacerse cargo de la secretaría de la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) (artículo 14 de la propuesta) y publicar un informe anual sobre la situación de la ciberseguridad en la UE (artículo 15 de la propuesta), iii) prestar apoyo a la organización de revisiones interpares entre los Estados miembros (artículo 16 de la propuesta), iv) recopilar datos agregados sobre incidentes de los Estados miembros y publicar orientaciones técnicas (artículo 20, apartado 9, de la propuesta), y v) crear y mantener un registro de entidades que presten servicios transfronterizos (artículo 25 de la propuesta).

Por consiguiente, se solicitarán cinco ETC adicionales a partir de 2022 con un presupuesto para cubrir estos nuevos puestos que asciende a aproximadamente a 0,61 millones EUR al año (véase la ficha financiera separada para las agencias).

Por consiguiente, se solicitarán cinco ETC adicionales a partir de 2022 con el correspondiente presupuesto para cubrir estos nuevos puestos.

☐ La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo.

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

En millones EUR (al tercer decimal)

	Año **N** [52] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)	**TOTAL**

[52] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

Agentes temporales (categoría AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Agentes temporales (categoría AST)								
Agentes contractuales	0,160	0,160	0,160	0,160	0,160	0,160		
Expertos nacionales en comisión de servicios								**0,96**

TOTAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Necesidades de personal (ETC):

	Año **N** [53] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)	**TOTAL**
Agentes temporales (categoría AD)	3	3	3	3	3	3		**18**
Agentes temporales (categoría AST)								
Agentes contractuales	2	2	2	2	2	2		**12**

[53] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

Expertos nacionales en comisión de servicios								

TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Coste de otros gastos administrativos

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

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

En millones EUR (al tercer decimal)

RÚBRICA 7 del marco financiero plurianual	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
En la sede:								
Gastos de misión y representación	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Costes de conferencias y reuniones	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Comités[54]								
Estudios y asesoramiento								
Sistemas de información y gestión								

[54] Especifíquese el tipo de comité y el grupo al que pertenece.

Equipos y servicios de TIC[55]								
Otras líneas presupuestarias (*especifíquense, en su caso*)								
en Delegaciones de la Unión								
Gastos de misiones, conferencias y representación								
Formación adicional del personal								
Adquisición, alquiler y gastos asociados								
Equipos, mobiliario, suministros y servicios								
Subtotal para la RÚBRICA 7 del marco financiero plurianual	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] TIC: Tecnologías de la información y de las comunicaciones: debe consultarse DIGIT.

En millones EUR (al tercer decimal)

Al margen de la RÚBRICA 7 del marco financiero plurianual	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Gastos en asistencia técnica y administrativa (con exclusión del personal externo) con cargo a créditos operativos (antiguas líneas «BA»)								
- en la sede								
- en Delegaciones de la Unión								
Otros gastos de gestión destinados a investigación								
Otras líneas presupuestarias (*especifíquense, en su caso*)								
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual								

TOTAL RÚBRICA 7 y al margen de la RÚBRICA 7 del marco financiero plurianual	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Las necesidades en materia de créditos administrativos se cubrirán con los créditos ya destinados a la gestión de la acción o reasignados, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

3. Métodos de cálculo utilizados para estimar los costes

3.1 Recursos humanos

En el presente apartado se recoge el método de cálculo utilizado para estimar los recursos humanos que se consideran necesarios [hipótesis del volumen de trabajo, incluidos puestos de trabajo específicos (perfiles de trabajo de Sysper 2), categorías de personal y los correspondientes costes medios]

RÚBRICA 7 del marco financiero plurianual
Nota: Los costes medios de cada categoría de personal en la sede están disponibles en BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Funcionarios y agentes temporales Seis funcionarios ETC (coste medio 0,150) = 0,9 por año - Elaboración de actos delegados de conformidad con el artículo 18, apartado 6, el artículo 21, apartado 2, y el artículo 36. - Elaboración de actos de ejecución de conformidad con el artículo 12, apartado 8, el artículo 18, apartado 5, y el artículo 20, apartado 11. - Proporcionar una secretaría para el Grupo de Cooperación SRI. - Organización de las reuniones plenarias y las reuniones de las líneas de trabajo del Grupo de Cooperación SRI. - Coordinación del trabajo de los Estados miembros en diversos documentos (directrices, herramientas, etc.). - Ejercer de enlace con otros servicios de la Comisión, la ENISA y las autoridades nacionales con vistas a la aplicación de la Directiva SRI. - Análisis de buenas prácticas y métodos nacionales relacionados con la aplicación de la Directiva SRI.
• Personal externo Tres AC (coste medio 0,08) = 0,24 por año - Apoyo a todas las funciones anteriores según proceda

Al margen de la RÚBRICA 7 del marco financiero plurianual
• Únicamente puestos financiados con cargo al presupuesto de investigación
• Personal externo

3.2 Otros gastos administrativos

Detállese el método de cálculo utilizado para cada línea presupuestaria

y, en particular, las hipótesis subyacentes (p. ej., número de reuniones al año, costes medios, etc.)

RÚBRICA 7 del marco financiero plurianual
Reuniones: las reuniones plenarias del Grupo de Cooperación SRI se suelen celebrar cuatro veces al año. La Comisión sufraga los gastos asociados al *catering* y los gastos de desplazamiento de representantes de veintisiete Estados miembros (un representante por cada uno de ellos). Los costes de una reunión pueden alcanzar los 15 000 EUR, lo que supone 60 000 EUR al año. Misiones: las misiones están relacionadas con el seguimiento de la aplicación de la Directiva SRI. Ejemplo: En un año (mayo de 2019 a julio de 2020), estaba previsto organizar las denominadas visitas en el contexto de la SRI y visitar a los veintisiete Estados miembros para analizar la aplicación de la Directiva SRI en toda la UE.

Al margen de la RÚBRICA 7 del marco financiero plurianual

ANEXO 7

de la
DECISIÓN DE LA COMISIÓN

sobre las normas internas de ejecución del presupuesto general de la Unión Europea (Sección de la Comisión Europea) a la atención de los servicios de la Comisión

FICHA FINANCIERA LEGISLATIVA «AGENCIAS»

La presente ficha financiera legislativa abarca la solicitud de reforzar el personal de la ENISA con cinco ETC a partir de 2022 para ejercer actividades adicionales asociadas a la aplicación de la Directiva SRI. Estas actividades ya están amparadas por el mandato de la ENISA.

Índice

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

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

Redes de Comunicación, Contenido y Tecnologías

1.3. La propuesta se refiere a

☐ **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto/una acción preparatoria**[56]

☒ **la prolongación de una acción existente**

☐ **una fusión o reorientación de una o más acciones hacia otra/una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

El objetivo de la revisión es incrementar el nivel de ciberresiliencia de un conjunto exhaustivo de empresas que operan en la Unión Europea en todos los sectores pertinentes, reducir las incoherencias en términos de resiliencia en todo el mercado interior en los sectores que ya están cubiertos por la Directiva y mejorar el nivel de conciencia situacional conjunta y la capacidad colectiva de preparación y respuesta.

1.4.2. Objetivo(s) específico(s)

A fin de resolver el problema del escaso nivel de ciberresiliencia de las empresas que operan en la Unión Europea, el objetivo específico consiste en garantizar que las entidades de todos los sectores que dependan de redes y sistemas de información y que presten servicios clave a la economía y la sociedad en su conjunto estén obligadas a adoptar medidas de ciberseguridad y notificar los incidentes con vistas a incrementar el nivel general de ciberresiliencia en todo el mercado interior.

Para solucionar el problema de la desigualdad en términos de resiliencia entre los Estados miembros y los sectores, el objetivo específico es velar por que todas las entidades activas en sectores amparados por el marco jurídico de la SRI y que sean de un tamaño similar y desempeñen una función comparable estén sujetas al mismo régimen reglamentario (ya sea dentro o fuera del ámbito de aplicación), con independencia de la jurisdicción a la que estén sometidas dentro de la UE.

Con el objetivo de garantizar que todas las entidades activas en los sectores amparados por el marco jurídico SRI deban cumplir las mismas obligaciones sobre la base del concepto de gestión de riesgos por lo que respecta a las medidas de seguridad y deban notificar todos los incidentes en función de un conjunto uniforme de criterios, los objetivos específicos consisten en velar por que las autoridades competentes hagan cumplir las normas establecidas en el

[56] Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero.

instrumento jurídico de manera más efectiva a través de medidas de supervisión y ejecución armonizadas, y en garantizar que los distintos Estados miembros destinen un nivel comparable de recursos a las autoridades competentes que les permita desempeñar las tareas básicas establecidas por el marco SRI.

A efectos de solucionar el problema de la conciencia situacional conjunta y la falta de respuesta conjunta a las crisis, el objetivo específico es garantizar que los Estados miembros intercambien información esencial mediante la introducción de unas obligaciones claras para que las autoridades competentes intercambien información y cooperen por lo que respecta a las ciberamenazas y los incidentes y el desarrollo de una capacidad operativa conjunta de respuesta a crisis en la Unión.

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener en los beneficiarios/grupos destinatarios.

Se prevé que la propuesta aporte beneficios significativos: según las estimaciones, podría reducir el coste de los incidentes de ciberseguridad en 11 300 millones EUR. El ámbito de aplicación sectorial del marco SRI se ampliaría considerablemente, pero además de los beneficios mencionados, la carga que los requisitos SRI podrían crear, en particular desde el punto de vista de la supervisión, también se equilibraría tanto para las nuevas entidades cubiertas como para las autoridades competentes. La razón es que el nuevo marco SRI establecería un enfoque en dos niveles, centrado en las entidades grandes y clave y con un régimen de supervisión diferenciado que permite aplicar únicamente supervisión *a posteriori* para un gran número de ellas, en particular las que se consideran «importantes», pero no «esenciales».

En general, la propuesta produciría compensaciones y sinergias eficientes, con el mejor potencial de todas las opciones de actuación analizadas para garantizar un nivel reforzado y coherente de ciberresiliencia de las entidades clave de toda la Unión que, en última instancia, se traduciría en ahorro de costes tanto para las empresas como para la sociedad.

Asimismo, la propuesta conllevaría determinados costes de conformidad y de ejecución para las autoridades competentes de los Estados miembros (se ha estimado un incremento general de entre el 20 y el 30 % aproximadamente). No obstante, el nuevo marco también entrañaría beneficios sustanciales gracias a una mejora de la visión general de las empresas clave y la interacción con ellas, el refuerzo de la cooperación operativa transfronteriza, así como mecanismos de asistencia mutua y revisión interpares. Con todo ello se produciría un aumento general de las capacidades de ciberseguridad en todos los Estados miembros.

Por lo que respecta a las empresas que estuviesen incluidas en el ámbito de aplicación del marco SRI, se calcula que tendrían que incrementar su gasto actual en seguridad informática en un 22 % como máximo durante los primeros años posteriores a la introducción del nuevo marco SRI (un 12 % en el caso de las empresas que ya están incluidas en el ámbito de aplicación de la Directiva SRI vigente). Aun así, este incremento medio del gasto en seguridad informática produciría un beneficio proporcional a dichas inversiones, en particular como consecuencia de la reducción considerable del coste de los incidentes de ciberseguridad (que según las estimaciones ascienden a 118 000 millones EUR a lo largo de diez años).

Las microempresas y las pequeñas empresas estarían excluidas del ámbito de aplicación del marco SRI. En lo tocante a las empresas medianas, cabe esperar que se produjese un aumento del nivel de gasto en seguridad de las TIC durante los primeros años posteriores a la introducción del nuevo marco SRI. Al mismo tiempo, el endurecimiento de los requisitos de seguridad aplicables a estas entidades también incentivaría sus capacidades de ciberseguridad y ayudaría a mejorar su gestión de los riesgos relacionados con las TIC.

Habría repercusiones en los presupuestos y las administraciones nacionales: cabe prever un aumento aproximado de entre el 20 y el 30 % de los recursos a corto y medio plazo.

No se contempla ninguna otra repercusión negativa significativa. Se espera que la propuesta promueva unas capacidades de ciberseguridad más sólidas y, por tanto, tendría un efecto de mitigación más sustancial en el número y la gravedad de los incidentes, incluidas las violaciones de la seguridad de los datos. Asimismo, es probable que tenga una repercusión positiva al garantizar unas condiciones de competencia equitativas en todos los Estados

miembros para todas las entidades incluidas en el ámbito de aplicación del marco SRI y reduzca las asimetrías en el ámbito de la información sobre ciberseguridad.

1.4.4. Indicadores de rendimiento

Especifíquense los indicadores que permiten realizar el seguimiento de los avances y los logros.

La evaluación de los indicadores será efectuada por la Comisión, con el apoyo de la ENISA y el Grupo de cooperación, por primera vez a los tres años de la entrada en vigor del nuevo acto jurídico SRI. Entre los indicadores de seguimiento que servirían para evaluar el éxito de la revisión del marco SRI cabe destacar:

- La mejora de la gestión de los incidentes: al adoptar medidas de ciberseguridad, las empresas no solo mejoran su capacidad para evitar del todo determinados incidentes, sino también su capacidad para responder a ellos. Por consiguiente, las medidas del éxito son i) la reducción del tiempo medio que transcurre hasta que se detecta un incidente, ii) el tiempo medio que necesitan las organizaciones para recuperarse de un incidente, y iii) el coste medio de los daños causados por un incidente.

- Una mayor conciencia de los riesgos de ciberseguridad entre la alta dirección de las empresas: al obligar a las empresas a adoptar medidas, con una Directiva SRI revisada se contribuiría a concienciar a la alta dirección sobre los riesgos relacionados con la ciberseguridad. Este aspecto puede medirse mediante el estudio de la medida en que las empresas incluidas en el ámbito de aplicación del marco SRI priorizan la ciberseguridad en sus políticas y procesos internos, a juzgar por su documentación interna y los programas de formación y actividades de concienciación pertinentes para los empleados, y priorizan la inversión en seguridad informática. Asimismo, la dirección de todas las entidades esenciales e importantes debe estar al tanto de las normas establecidas en la Directiva SRI.

- El equilibrio del gasto sectorial: el gasto en seguridad informática varía considerablemente de un sector a otro en la UE. Al exigir que empresas de más sectores adopten medidas, las desviaciones del gasto medio sectorial en seguridad informática como porcentaje del gasto global en TIC debería disminuir entre sectores y en todos los Estados miembros.

- El refuerzo de las autoridades competentes y el aumento de la cooperación: una Directiva SRI revisada podría conferir funciones adicionales a las autoridades competentes. Esto tendría una repercusión cuantificable en los recursos financieros y humanos dedicados a las agencias de ciberseguridad a escala nacional y también debería tener un impacto positivo en la capacidad de las autoridades competentes para cooperar de manera proactiva y, por tanto, aumentar el número de casos en que las autoridades competentes interactúan entre sí a efectos de abordar los incidentes transfronterizos o realizar actividades conjuntas de supervisión.

- El aumento del intercambio de información: el marco SRI revisado también mejoraría el intercambio de información entre empresas y con las autoridades competentes. Una de las metas de la revisión podría ser incrementar el número de entidades que participan en las diversas formas de intercambiar información.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado para la aplicación de la iniciativa

El objetivo de la propuesta es incrementar el nivel de ciberresiliencia de un conjunto exhaustivo de empresas que operan en la Unión Europea en todos los sectores pertinentes,

reducir las incoherencias en términos de resiliencia en todo el mercado interior en los sectores que ya están cubiertos por la Directiva y mejorar el nivel de conciencia situacional conjunta y la capacidad colectiva de preparación y respuesta. Partirá de los logros alcanzados con la aplicación de la Directiva (UE) 2016/1148 durante los últimos cuatro años.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como una mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, por «valor añadido de la intervención de la Unión» se entenderá el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

La resiliencia en términos de ciberseguridad en toda la Unión no puede ser eficaz si se aplican distintos enfoques de carácter nacional o regional. La Directiva SRI solucionó esta deficiencia al establecer un marco para la seguridad de las redes y los sistemas de información a escala nacional y de la Unión. No obstante, la primera revisión periódica de la Directiva SRI señaló una serie de fallos inherentes que, en última instancia, han culminado en disparidades considerables entre los Estados miembros en términos de capacidades, planificación y nivel de protección que afectan al mismo tiempo a las condiciones de competencia equitativas para empresas similares en el mercado interior.

Los siguientes motivos justifican que la intervención de la UE trascienda las medidas actuales de la Directiva SRI: i) la naturaleza transfronteriza del problema; ii) el potencial de que la intervención de la UE mejore unas políticas nacionales efectivas y las facilite; y iii) la contribución de unas acciones políticas concertadas y colaborativas a la protección efectiva de los datos y la privacidad.

De esta manera, los objetivos indicados pueden alcanzarse mejor a través de la actuación de la Unión que por los Estados miembros en solitario.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La Directiva SRI es el primer instrumento horizontal del mercado interior destinado a mejorar la resiliencia de las redes y los sistemas en la Unión frente a los riesgos de ciberseguridad. Desde su entrada en vigor en 2016, ya ha contribuido en gran medida a aumentar el nivel común de ciberseguridad entre los Estados miembros. No obstante, la revisión del funcionamiento y la aplicación de la Directiva han puesto de manifiesto varias deficiencias que, además del aumento de la digitalización y la necesidad de una respuesta más actualizada, deben subsanarse en un acto jurídico revisado.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

La nueva propuesta es plenamente coherente y consecuente con otras iniciativas relacionadas, como la propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero y la propuesta de Directiva sobre la resiliencia de los operadores críticos de servicios esenciales. Asimismo, es coherente con el Código Europeo de las Comunicaciones Electrónicas, el Reglamento General de Protección de Datos y el Reglamento eIDAS.

La propuesta es un componente fundamental de la Estrategia de la UE para una Unión de la Seguridad.

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

La gestión de estas funciones por parte de la ENISA requiere perfiles específicos y un volumen de trabajo adicional que no puede absorberse sin un refuerzo de los recursos humanos.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

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

– ☐ Incidencia financiera desde AAAA hasta AAAA

☒ **duración ilimitada**

– Ejecución con una fase de puesta en marcha desde 2022 hasta 2025,

– y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[57]

☒ **Gestión directa** a cargo de la Comisión

a través de

– ☐ agencias ejecutivas

☐ **Gestión compartida** con los Estados miembros

☐X **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

☐ organizaciones internacionales y sus agencias (especifíquense);

☐ el Banco Europeo de Inversiones (BEI) y el Fondo Europeo de Inversiones;

☒ los organismos contemplados en los artículos 70 y 71;

☐ organismos de Derecho público;

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

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

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

Observaciones

La Agencia de la Unión Europea para la Ciberseguridad (ENISA), a la que se ha otorgado un nuevo mandato permanente a través del Reglamento sobre la Ciberseguridad, prestaría asistencia a los Estados miembros y a la Comisión en la aplicación de la Directiva SRI revisada.

Como resultado de la Directiva SRI revisada, a partir del año 2022/2023, la ENISA tendrá ámbitos de actuación adicionales. Aunque estos ámbitos de actuación estarían cubiertos por las funciones generales de la ENISA de acuerdo con su mandato, se traducirán en un aumento de la carga de trabajo para la Agencia. Más concretamente, aparte de sus ámbitos de actuación actuales, en virtud de la propuesta de la Comisión de Directiva SRI revisada la ENISA deberá también incorporar específicamente a su programa de trabajo las siguientes funciones a título ilustrativo: i) desarrollar y

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

mantener un Registro Europeo de Vulnerabilidades (artículo 6, apartado 2, de la propuesta), ii) hacerse cargo de la secretaría de la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) (artículo 14 de la propuesta) y publicar un informe anual sobre la situación de la ciberseguridad en la UE (artículo 15 de la propuesta), iii) prestar apoyo a la organización de revisiones interpares entre los Estados miembros (artículo 16 de la propuesta), iv) recopilar datos agregados sobre incidentes de los Estados miembros y publicar orientaciones técnicas (artículo 20, apartado 9, de la propuesta), y v) crear y mantener un registro de entidades que presten servicios transfronterizos (artículo 25 de la propuesta).

Por consiguiente, se solicitarán cinco ETC adicionales a partir de 2022 con un presupuesto para cubrir estos nuevos puestos que asciende a aproximadamente 0,61 millones EUR al año.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

La Comisión revisará periódicamente el funcionamiento de la Directiva e informará al Parlamento Europeo y al Consejo, por primera vez tres años después de la entrada en vigor.

Asimismo, la Comisión evaluará la correcta transposición de la Directiva por parte de los Estados miembros.

El seguimiento de la propuesta y la elaboración de informes al respecto se regirán por los principios recogidos en el mandato permanente de la ENISA en virtud del Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad»).

Las fuentes de datos utilizadas para el seguimiento previsto procederían en su mayoría de la ENISA, el Grupo de cooperación, la red de CSIRT y las autoridades de los Estados miembros. Además de los datos recopilados a partir de los informes (incluidos los informes anuales de actividad) de la ENISA, el Grupo de Cooperación y la red de CSIRT, podrían utilizarse herramientas específicas de recopilación de datos en caso de ser necesario (p. ej., encuestas a las autoridades nacionales, Eurobarómetro e informes de la campaña del Mes de la Ciberseguridad y los ejercicios paneuropeos).

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

La unidad de la DG CNECT responsable del ámbito político gestionará la aplicación de la Directiva.

Por lo que respecta a la gestión de la ENISA, el artículo 15 del Reglamento sobre la Ciberseguridad contempla una lista detallada de las funciones de control del Consejo de Administración de la ENISA.

Al amparo del artículo 31 de dicho Reglamento, el director ejecutivo de la ENISA es el responsable de la ejecución del presupuesto de la Agencia y el auditor interno de la Comisión ejerce, con respecto a la ENISA, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión. El Consejo de Administración de la ENISA emite un dictamen sobre las cuentas definitivas de la Agencia.

2.2.2. Información relativa a los riesgos identificados y al sistema o los sistemas de control interno establecidos para mitigarlos

Riesgo muy bajo, puesto que el ecosistema de la Directiva SRI ya está instaurado y abarca a la ENISA, que tiene un mandato permanente tras la entrada en vigor del Reglamento sobre la Ciberseguridad en 2019.

2.2.3. Estimación y justificación de la rentabilidad de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados») y evaluación del nivel de riesgo de error previsto (al pago y al cierre)

El incremento presupuestario solicitado aplica el título 1 y está destinado a financiar salarios, lo que implica un riesgo muy bajo de error a nivel de pago.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

Se aplicarían las medidas de prevención y protección de la ENISA, concretamente:

- Los pagos por cualquier servicio o estudio solicitado son comprobados por el personal de la Agencia antes del pago, teniendo en cuenta las obligaciones contractuales, los principios económicos y las buenas prácticas financieras o de gestión. Se incluirán disposiciones antifraude (supervisión, requisitos de notificación, etc.) en todos los acuerdos y contratos celebrados entre la Agencia y los beneficiarios de cualquier pago.

- Para luchar contra el fraude, la corrupción y cualesquiera otras prácticas contrarias a Derecho, se aplicarán sin restricciones las disposiciones del 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.

- En virtud del artículo 33 del Reglamento sobre la Ciberseguridad, antes del 28 de diciembre de 2019, la ENISA suscribió 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). La ENISA publicará, sin demora, las disposiciones apropiadas aplicables a todo el personal de la Agencia.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

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

- Líneas presupuestarias existentes

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

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[58]	de países de la AELC[59]	de países candidatos [60]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
2	02 10 04	/CND	SÍ	NO	NO	/NO

- Nuevas líneas presupuestarias solicitadas

[58] CD = créditos disociados / CND = créditos no disociados.
[59] AELC: Asociación Europea de Libre Comercio.
[60] Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales.

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

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND	de países de la AELC	de países candidatos	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
	[XX.YY.YY.YY]		SÍ/NO	SÍ/NO	SÍ/NO	SÍ/NO

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	[Rúbrica…2 Mercado único, innovación y economía digital……...……]

[Organismo]: <…ENISA….>			Año **N**[61] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6) **2026**	**2027**		**TOTAL**
Título 1:	Compromisos	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Pagos	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Título 2:	Compromisos	(1a)								
	Pagos	(2a)								
Título 3:	Compromisos	(3a)								
	Pagos	(3b)								
TOTAL de los créditos para el [organismo] <ENISA…….>	Compromisos	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Pagos	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

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

En millones EUR (al tercer decimal)

		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
DG: <…….>									
• Recursos humanos									
• Otros gastos administrativos									
TOTAL para la DG <…….>	Créditos								

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = total de los pagos)								

En millones EUR (al tercer decimal)

		Año **N**[62] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6) **2026**	**2027**		**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Pagos	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

3.2.2. Incidencia estimada en los créditos de [organismo]

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

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

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⇩			Año **N**		Año **N+1**		Año **N+2**		Año **N+3**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
	RESULTADOS																	
	Tipo[63]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.º 1[64]…																		
- Resultado																		
- Resultado																		
- Resultado																		
Subtotal del objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2																		
- Resultado																		
Subtotal del objetivo específico n.º 2																		
COSTE TOTAL																		

63 Los resultados son productos y servicios que deben suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

64 Tal como se describe en el punto 1.4.2, titulado. «Objetivo(s) específico(s)».

3.2.3. Incidencia estimada en los recursos humanos de la ENISA

3.2.3.1. Resumen

Como resultado de la Directiva SRI revisada, a partir del año 2022/2023, la ENISA se encargará de tareas adicionales. Aunque estas funciones estarían cubiertas por el mandato de la ENISA, se traducirán en un aumento de la carga de trabajo para la Agencia. Más concretamente, además de las funciones que realiza en la actualidad, en virtud de la propuesta de la Comisión de Directiva SRI revisada, la ENISA se encargará, entre otros, de i) desarrollar y mantener un Registro Europeo de Vulnerabilidades (artículo 6, apartado 2), ii) hacerse cargo de la secretaría de la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) (artículo 14) y publicar un informe anual sobre la situación de la ciberseguridad en la UE (artículo 15), iii) prestar apoyo a la organización de revisiones interpares entre los Estados miembros (artículo 16), iv) recopilar datos agregados sobre incidentes de los Estados miembros y publicar orientaciones técnicas (artículo 20, apartado 9), y v) crear y mantener un registro de entidades que presten servicios transfronterizos (artículo 25).

Por consiguiente, se solicitarán cinco ETC adicionales a partir de 2022 con el correspondiente presupuesto para cubrir estos nuevos puestos.

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

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

En millones EUR (al tercer decimal)

	Año **N**[65] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6) **2026** **2027**			**TOTAL**
Agentes temporales (categoría AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Agentes temporales (categoría AST)								
Agentes contractuales	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Expertos nacionales en comisión de servicios								

65 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

TOTAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Necesidades de personal (ETC):

	Año **N**[66] **2022**	Año **N+1** **2023**	Año **N+2** **2024**	Año **N+3** **2025**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6) **2026** **2027**			**TOTAL**
Agentes temporales (categoría AD)	3	3	3	3	3	3		**18**
Agentes temporales (categoría AST)								
Agentes contractuales	2	2	2	2	2	2		**12**
Expertos nacionales en comisión de servicios								
TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Necesidades estimadas de recursos humanos para la DG matriz

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

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

La estimación debe expresarse en importes íntegros (o, como mínimo, al primer decimal)

	Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
• **Empleos de plantilla (funcionarios y personal temporal)**							
XX 01 01 01 (sede y oficinas de Representación de la Comisión)							
XX 01 01 02 (Delegaciones)							
XX 01 05 01 (investigación indirecta)							

66 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de ejecución previsto (por ejemplo: 2021). Repítase con los años siguientes.

10 01 05 01 (investigación directa)								
• **Personal externo [en equivalente a tiempo completo (ETC)]**[67]								
XX 01 02 01 (AC, ENCS, INT de la dotación global)								
XX 01 02 02 (AC, AL, ENCS, INT y JPD en las Delegaciones)								
XX 01 04 ***yy***[68]	- en la sede[69]							
	- en las Delegaciones							
XX 01 05 02 (AC, ENCS, INT; investigación indirecta)								
10 01 05 02 (AC, ENCS, INT; investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL								

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	
Personal externo	

En el anexo V, sección 3, debe incluirse una descripción del cálculo del coste de las unidades de ETC.

67 AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD = joven profesional en delegación.

68 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

69 Principalmente para los Fondos Estructurales, el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) y el Fondo Europeo de Pesca (FEP).

3.2.4. Compatibilidad con el marco financiero plurianual vigente

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

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

Explíquese la reprogramación requerida, precisando las líneas presupuestarias afectadas y los importes correspondientes. La propuesta es compatible con el MFP 2021-2027. La compensación del presupuesto solicitado para cubrir el incremento de recursos de RR. HH. en la ENISA se logrará al reducir en la misma medida el presupuesto del programa Europa Digital en la misma rúbrica.

– ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[70].

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes.

3.2.5. Contribución de terceros

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

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

En millones EUR (al tercer decimal)

	Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

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

3.3. Incidencia estimada en los ingresos

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

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

☐ en los recursos propios

☐ en otros ingresos

☐ indíquese si los ingresos se asignan a líneas de gasto

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[71]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo ….								

En el caso de los ingresos diversos «asignados», especifíquense la línea o líneas presupuestarias de gasto en la(s) que repercutan.

Especifíquese el método de cálculo de la incidencia en los ingresos.

[71] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos una vez deducido el 20 % de los gastos de recaudación.