COMUNICACIÓN DE LA COMISIÓN

Directrices de la Comisión sobre la aplicación del artículo 4, apartados 1 y 2, de la Directiva (UE) 2022/2555 (Directiva SRI 2)

(2023/C 328/02)

I. INTRODUCCION

1. De conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2) ([1]), la Comisión proporcionará, a más tardar el 17 de julio de 2023, directrices que aclaren la aplicación de los apartados 1 y 2 del artículo 4 de dicha Directiva.

2. Las presentes Directrices aclaran la aplicación de dichas disposiciones, que se refieren a la relación entre la Directiva (UE) 2022/2555 y los actos jurídicos sectoriales actuales y futuros de la Unión que abordan las medidas para la gestión de riesgos de ciberseguridad o los requisitos de notificación de incidentes. El apéndice de estas Directrices enumera los actos jurídicos sectoriales de la Unión que la Comisión considera que entran en el ámbito de aplicación del artículo 4 de la Directiva (UE) 2022/2555. El hecho de que un acto no figure en dicho apéndice no significa necesariamente que no entre en el ámbito de aplicación de esa disposición.

3. De conformidad con el artículo 4, apartado 3, tercera frase, de la Directiva (UE) 2022/2555, la Comisión ha tenido en cuenta las observaciones del Grupo de cooperación SRI y de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) antes de la adopción de estas Directrices.

4. Las presentes Directrices se entienden sin perjuicio de la interpretación del Derecho de la Unión que realice el Tribunal de Justicia de la Unión Europea.

II. EQUIVALENCIA DE LOS REQUISITOS DE CIBERSEGURIDAD DE LOS ACTOS JURÍDICOS SECTORIALES DE LA UNIÓN

5. El artículo 4, apartado 1, de la Directiva (UE) 2022/2555 establece que, cuando los actos jurídicos sectoriales de la Unión requieran que las entidades esenciales o importantes adopten medidas para la gestión de riesgos de ciberseguridad o notifiquen los incidentes significativos y cuando dichos requisitos tengan un efecto al menos equivalente al de las obligaciones establecidas en la presente Directiva, no se aplicarán a estas entidades las disposiciones pertinentes de la Directiva (UE) 2022/2555, incluidas las relativas a la supervisión y la garantía del cumplimiento recogidas en el capítulo VII. Esa disposición establece además que cuando los actos jurídicos sectoriales de la Unión no cubran a todas las entidades de un sector concreto incluidas en el ámbito de aplicación de Directiva (UE) 2022/2555, las disposiciones pertinentes de la presente Directiva seguirán aplicándose a las entidades no cubiertas por los actos jurídicos sectoriales de la Unión en cuestión.

II.1. Requisitos de gestión de riesgos de ciberseguridad

6. El artículo 4, apartado 2, letra a), de la Directiva (UE) 2022/2555 establece que, las medidas para la gestión de riesgos de ciberseguridad que las entidades esenciales o importantes estén obligadas a adoptar en virtud de actos jurídicos sectoriales de la Unión se considerarán equivalentes en sus efectos a las obligaciones establecidas en la Directiva (UE) 2022/2555 cuando dichas medidas sean al menos equivalentes en sus efectos a las previstas en el artículo 21, apartados 1 y 2, de dicha Directiva. Al evaluar si los requisitos de un acto jurídico sectorial de la Unión sobre las medidas para la gestión de riesgos en materia de ciberseguridad tengan un efecto al menos equivalente en sus efectos a las previstas en el artículo 21, apartados 1 y 2, de la Directiva (UE) 2022/2555, los requisitos de dicho acto jurídico sectorial de la Unión deben, como mínimo, corresponder a los requisitos de dichas disposiciones o ir más allá, lo que significa que las disposiciones sectoriales pueden ser más detalladas en cuanto al fondo en comparación con las disposiciones correspondientes de la Directiva (UE) 2022/2555.

([1]) DO L 333 de 27.12.2022, p. 80.

7. De conformidad con el artículo 21, apartado 1, párrafo primero, de la Directiva (UE) 2022/2555, los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios. Estas medidas deben basarse en el riesgo y ser capaces de prevenir o minimizar las repercusiones de los incidentes. El artículo 21, apartado 1, párrafo segundo, de la Directiva (UE) 2022/2555 especifica cómo debe evaluarse la proporcionalidad de tales medidas ([2]). La obligación establecida en el artículo 21, apartado 1, de la Directiva (UE) 2022/2555, por la que se exige a las entidades esenciales e importantes que adopten medidas adecuadas y proporcionadas de gestión de los riesgos en materia de ciberseguridad, se refiere a todas las operaciones y servicios de la entidad en cuestión, y no solo a los activos específicos de tecnología de la información («TI») o a los servicios esenciales que presta la entidad.

8. Al evaluar la equivalencia de un acto jurídico sectorial de la Unión con las disposiciones pertinentes sobre la gestión de riesgos en materia de ciberseguridad de la Directiva (UE) 2022/2555, debe concederse especial importancia a la cuestión de si las obligaciones de seguridad de dicho acto jurídico incluyen medidas destinadas a garantizar la seguridad de las redes y los sistemas de información. La definición de «seguridad de los sistemas de redes y de información» establecida en el artículo 6, punto 2 de la Directiva (UE) 2022/2555 se refiere a la capacidad de los sistemas de redes y de información de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos. El uso de los términos «disponibilidad», «autenticidad», «integridad» y «confidencialidad» en esa definición se refiere a los cuatro objetivos de protección relacionados con la seguridad de los sistemas de redes y de información. El término «sistemas de redes y de información», tal como se define en el artículo 6, punto 1 de la Directiva (UE) 2022/2555, incluye las redes de comunicaciones electrónicas ([3]); todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, conforme a un programa, el tratamiento automático de datos digitales; y los datos digitales almacenados, tratados, recuperados o transmitidos por dichas redes de comunicaciones electrónicas o dispositivos para su funcionamiento, utilización, protección y mantenimiento. Por consiguiente, las medidas de seguridad exigidas por un acto jurídico sectorial de la Unión deben comprender también el soporte material, los microprogramas y los programas informáticos utilizados en las actividades de una entidad.

9. Otra consideración importante a la hora de determinar la equivalencia de un acto jurídico sectorial de la Unión con los requisitos del artículo 21, apartados 1 y 2, de la Directiva (UE) 2022/2555 es que las medidas de gestión de riesgos de ciberseguridad exigidas por dicho acto deben basarse en un «planteamiento que abarque todos los riesgos». Dado que las amenazas a la seguridad de los sistemas de redes y de información pueden tener distintos orígenes, cualquier tipo de evento puede tener un impacto negativo en las redes y los sistemas de información de la entidad y conducir potencialmente a un incidente. Por lo tanto, las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad deben proteger no solo las redes y los sistemas de información de una entidad, sino también el entorno físico de dichos sistemas frente a cualquier suceso, como sabotajes, robos, incendios, inundaciones, fallos en las telecomunicaciones o de suministro de la electricidad, o acceso físico no autorizado, que puedan poner en peligro la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. Por consiguiente, las medidas para la gestión de riesgos de ciberseguridad exigidas por un acto jurídico sectorial de la Unión deben abordar específicamente la seguridad física y de los entornos de redes y sistemas de información frente a fallos del sistema, errores humanos, actos malintencionados o fenómenos naturales ([4]).

10. El artículo 21, apartado 2, de la Directiva (UE) 2022/2555 exige además que las medidas de gestión de riesgos de ciberseguridad incluyan los requisitos específicos de seguridad enumerados en las letras a) a j) del apartado 2 de dicha disposición. Estos requisitos abarcan medidas como las políticas de seguridad de los sistemas de información y análisis de riesgos, la gestión de incidentes, la continuidad de la actividad, la gestión de crisis, la seguridad de la cadena de suministro, las políticas y procedimientos relativos al uso de criptografía y, en su caso, de cifrado. Con arreglo al artículo 21, apartado 5, párrafo segundo, de la Directiva (UE) 2022/2555, la Comisión está facultada para adoptar actos de ejecución por los que se establezcan los requisitos técnicos y metodológicos, así como los

([2]) Véanse también los considerandos 78, 81 y 82 de la Directiva (UE) 2022/2555.

([3]) Artículo 2, apartado 1, de la 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).

([4]) Véase el considerando 79 de la Directiva (UE) 2022/2555.

requisitos sectoriales, según sea necesario, de las medidas de seguridad a que se refiere el artículo 21, apartado 2, de dicha Directiva. Por lo que respecta a los proveedores de servicios de sistema de nombres de dominio («DNS»), los registros de nombres de dominio de primer nivel («TLD»), los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionada, los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza, la Comisión adoptará, a más tardar el 17 de octubre de 2024, actos de ejecución sobre los requisitos técnicos y metodológicos de las medidas de seguridad a que se refiere el artículo 21, apartado 2, de la Directiva (UE) 2022/2555. Los actos de ejecución especifican con mayor detalle las principales condiciones y criterios de ejecución establecidos en el acto de base, sin que ello afecte a la esencia de dicho acto ([5]).

II.2. **Requisitos de comunicación de información**

11. El artículo 4, apartado 2, letra b), de la Directiva (UE) 2022/2555 establece que los requisitos de comunicación de información sobre la notificación de incidentes significativos se considerarán equivalentes en sus efectos a las obligaciones de dicha Directiva cuando un acto jurídico sectorial de la Unión prevea el acceso inmediato, y cuando proceda automático y directo, a las notificaciones de incidentes por parte de los de los equipos de respuesta a incidentes de seguridad informática («CSIRT»), las autoridades competentes o puntos de contacto únicos («SPOC»), y cuando los requisitos de notificación de incidentes significativos tengan un efecto al menos equivalente a los establecidos en el artículo 23, apartados 1 a 6 de la Directiva (UE) 2022/2555.

12. Dado que los requisitos de un acto jurídico sectorial de la Unión para los requisitos de notificación de incidentes significativos deben tener un efecto al menos equivalente a los establecidos en el artículo 23, apartados 1 a 6 de la Directiva (UE) 2022/2555 para que dicho acto se aplique en lugar de las obligaciones de notificación de dicha Directiva, los requisitos establecidos en el artículo 23, apartados 1 a 6, de la Directiva revisten especial importancia para la evaluación de la equivalencia. Los apartados 1 a 6 del artículo 23 de la Directiva (UE) 2022/2555 prescriben con más detalle qué tipo de incidentes deben notificarse a quién, en qué plazo y con qué contenido informativo. Esto se explica más detalladamente en las subsecciones siguientes:

II.2.1. *Notificación de incidentes significativos a los CSIRT, las autoridades competentes y los destinatarios*

13. La primera frase del primer párrafo del apartado 1 del artículo 23 de la Directiva (UE) 2022/2555 exige que las entidades esenciales e importantes notifiquen, sin demora indebida, a su CSIRT o, en su caso, a su autoridad competente, cualquier incidente significativo. La segunda frase del primer párrafo del apartado 1 del artículo 23 de la Directiva (UE) 2022/2555 exige que las entidades esenciales e importantes notifiquen, en su caso, sin demora indebida, a los destinatarios de sus servicios los incidentes significativos susceptibles de afectar negativamente a la prestación de dichos servicios.

14. Mientras que el artículo 6, punto 6, de la Directiva (UE) 2022/2555 define los «incidentes» de forma muy amplia, como cualquier 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, el artículo 23, apartado 1, de dicha Directiva solo somete los incidentes significativos a una obligación de notificación. Un incidente es significativo si ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada [artículo 23, apartado 3, letra a)], ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables [artículo 23, apartado 3, letra b)].

([5]) Véase el capítulo D Normas adicionales de ejecución del acto de base, Criterios no vinculantes para la aplicación de los artículos 290 y 291 del Tratado de Funcionamiento de la Unión Europea —18 de junio de 2019 (DO C 223 de 3.7.2019, p. 1).

15. El considerando 101 de la Directiva (UE) 2022/2555 aclara que la notificación de incidentes debe basarse en una evaluación inicial realizada por la entidad afectada. Tal evaluación inicial debe tener en cuenta, entre otros aspectos, los sistemas de redes y de información afectados, y en particular su importancia para la prestación de los servicios de la entidad, la gravedad y las características técnicas de la ciberamenaza, cualquier vulnerabilidad subyacente que se esté aprovechando, así como la experiencia de la entidad con incidentes similares. Indicadores como la medida en que se ve afectado el funcionamiento del servicio, la duración de un incidente o el número de destinatarios de los servicios afectados podrían ser importantes a la hora de determinar si la perturbación operativa del servicio es grave.

16. De conformidad con el artículo 23, apartado 11, párrafo segundo, de la Directiva (UE) 2022/2555, la Comisión está facultada para adoptar actos de ejecución en los que se especifiquen los casos en que un incidente se considerará significativo. En lo que respecta a los proveedores de servicios de DNS, los registros de nombres del dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, la Comisión adoptará dichos actos de ejecución a más tardar el 17 de octubre de 2024. Los actos de ejecución especifican con mayor detalle las principales condiciones y criterios de ejecución establecidos en el acto de base, sin que ello afecte a la esencia de dicho acto ([6]).

II.2.2. *Enfoque en varias etapas y plazos para la notificación de incidentes significativos*

17. La Directiva (UE) 2022/2555 establece un enfoque en varias etapas respecto a la notificación de incidentes significativos que implica una alerta temprana, una notificación del incidente y un informe final. Estos tres elementos pueden completarse con informes intermedios y un informe de situación.

18. El enfoque en varias etapas tiene por objeto alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a reducir la posible propagación de incidentes significativos y permita a las entidades esenciales e importantes buscar asistencia, y, por el otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente y mejore con el tiempo la ciberresiliencia de las entidades individualmente y de sectores completos ([7]).

19. Según el enfoque en varias etapas, las entidades esenciales e importantes deben presentar en primer lugar una alerta temprana al CSIRT o autoridad competente y, en cualquier caso, en un plazo de veinticuatro horas desde que haya tenido constancia del incidente significativo. Posteriormente, dichas entidades deberán presentar una notificación del incidente, sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas desde que se haya tenido constancia del incidente significativo. A partir de ese momento, un CSIRT o autoridad competente podrá solicitar un informe intermedio. Por último, debe entregarse un informe final al CSIRT o a la autoridad competente en el plazo máximo de un mes desde la presentación de la notificación del incidente, a menos que el incidente siga en curso en ese momento, en cuyo caso debe entregarse un informe de situación y el informe final en el plazo de un mes a partir de que hayan gestionado el incidente.

20. Se aplica un plazo diferente para la notificación de incidentes establecida en el segundo párrafo del apartado 4 del artículo 23 de la Directiva (UE) 2022/2555 en relación con los proveedores de servicios de confianza. Dichos proveedores deben notificar los incidentes significativos en la prestación de sus servicios de confianza sin demora indebida y, en cualquier caso, en un plazo de veinticuatro horas desde que haya tenido constancia del incidente significativo.

([6]) Véase el capítulo D Normas adicionales de ejecución del acto de base, Criterios no vinculantes para la aplicación de los artículos 290 y 291 del Tratado de Funcionamiento de la Unión Europea —18 de junio de 2019 (DO C 223/1 de 3.7.2019, p. 1).

([7]) Véase el considerando 101 de la Directiva (UE) 2022/2555.

II.2.3. *Contenido de la obligación de notificación de incidentes significativos a los CSIRT o a las autoridades competentes*

21. Como norma general, la tercera frase del artículo 23, apartado 1, párrafo primero, de la Directiva (UE) 2022/2555 exige a los Estados miembros que garanticen que dichas entidades notifiquen, entre otros detalles, cualquier información que permita al CSIRT o, en su caso, a la autoridad competente determinar las repercusiones transfronterizas del incidente. Este requisito relativo al contenido de la obligación de informar se especifica con más detalle en el apartado 4 del artículo 23 de la Directiva (UE) 2022/2555, que establece el enfoque en varias etapas.

22. De conformidad con el artículo 23, apartado 4, letra a), la alerta temprana debe indicar si se sospecha que el incidente significativo está causado por actos ilícitos o malintencionados y si es probable que tenga repercusiones transfronterizas. Según el considerando 102 de la Directiva (UE) 2022/2555, la alerta temprana solo debe incluir la información necesaria para que el CSIRT, o, en su caso, la autoridad competente, tenga constancia del incidente significativo y la entidad afectada pueda solicitar asistencia, en caso de que sea necesario.

23. La notificación del incidente debe incluir, en su caso, actualizaciones de la información presentada en el marco de la alerta temprana. Además, debe incluir una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles.

24. En caso de que se solicite un informe intermedio, deberá incluir las actualizaciones de estado pertinentes. El informe final debe incluir una descripción detallada del incidente, incluyendo su gravedad e impacto, el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente, las medidas paliativas aplicadas y en curso y, cuando proceda, las repercusiones transfronterizas del incidente.

II.2.4. *Acceso inmediato a las notificaciones de incidentes*

25. El artículo 4, apartado 2, letra b), de la Directiva (UE) 2022/2555 establece que un acto jurídico sectorial de la Unión, para ser aplicable con respecto a los requisitos de notificación en lugar de dicha Directiva, debe proporcionar a los CSIRT, las autoridades competentes o los puntos de contacto únicos con arreglo a la Directiva (UE) 2022/2555 acceso inmediato a las notificaciones de incidentes presentadas de conformidad con el acto jurídico sectorial de la Unión. De conformidad con el considerando 24 de la Directiva (UE) 2022/2555, tal acceso inmediato puede garantizarse, en particular, si las notificaciones de incidentes se transmiten sin demora indebida al CSIRT, la autoridad competente o el punto de contacto único.

26. El acceso inmediato puede facilitarse a través de medios automáticos y directos que los Estados miembros deben establecer, en su caso. Los mecanismos de notificación automática y directa garantizan el intercambio sistemático e inmediato de información con los CSIRT, las autoridades competentes o los puntos de contacto únicos en relación con la tramitación de las notificaciones de incidentes. Los Estados miembros también pueden utilizar una ventanilla única que debe cumplir el acto jurídico sectorial de la Unión, para simplificar la notificación y aplicar el mecanismo de notificación automática y directa.

27. Al evaluar si los requisitos de un acto jurídico sectorial de la Unión para notificar incidentes significativos tengan un efecto al menos equivalente a los establecidos en el artículo 23, apartados 1 a 6 de la Directiva (UE) 2022/2555, los requisitos de dicho acto jurídico sectorial de la Unión deben, como mínimo, corresponder a los requisitos del artículo 23, apartados 1 a 6, o ser más detallados que esas disposiciones. Los requisitos deben referirse al tipo de incidentes que deben notificarse con arreglo a la Directiva (UE) 2022/2555, teniendo en cuenta, en particular, los destinatarios, el contenido y los plazos aplicables.

III. **EFECTOS DE LA EQUIVALENCIA**

III.1. **Medidas de supervisión y ejecución**

28. Cuando los actos jurídicos sectoriales de la Unión tengan al menos un efecto equivalente al de las obligaciones establecidas en la presente Directiva (UE) 2022/2555, no solo no se aplicarán las disposiciones pertinentes de dicha Directiva relativas a la obligación de adoptar medidas de gestión de riesgos en materia de ciberseguridad o de notificar incidentes significativos, así como las disposiciones sobre supervisión y ejecución establecidas en el capítulo VII de la Directiva (UE) 2022/2555.

29. El considerando 25 de la Directiva (UE) 2022/2555 explica que los actos jurídicos sectoriales de la Unión que tengan un efecto al menos equivalente podrían disponer que las autoridades competentes en virtud de dichos actos ejerzan sus facultades de supervisión y ejecución en relación con las obligaciones de gestión de riesgos o notificación en materia de ciberseguridad con la asistencia de las autoridades competentes en virtud de la Directiva (UE) 2022/2555. Las autoridades competentes afectadas podrían establecer acuerdos de cooperación a tal efecto, incluidos procedimientos relativos a la coordinación de las actividades de supervisión, los procedimientos para las investigaciones y la inspecciones *in situ* de conformidad con el Derecho nacional, así como un mecanismo de intercambio de información pertinente en materia de supervisión y ejecución entre las autoridades competentes. Este mecanismo de intercambio de información pertinente podría implicar el acceso a la información relacionada con la cibernética solicitada por las autoridades competentes en virtud de la Directiva (UE) 2022/2555.

III.2. **Estrategia nacional de ciberseguridad**

30. Cada Estado miembro ha de adoptar una estrategia nacional de ciberseguridad de conformidad con el artículo 7, apartado 1, de la Directiva (UE) 2022/2555. Una estrategia nacional de ciberseguridad es un marco coherente de un Estado miembro que establece prioridades y objetivos estratégicos en el ámbito de la ciberseguridad y la gobernanza para alcanzar estos objetivos y prioridades en dicho Estado miembro [véase el artículo 6, punto 4, de la Directiva (UE) 2022/2555]. La estrategia de ciberseguridad debe incluir, entre otras cosas, objetivos y prioridades que abarquen, en particular, los sectores mencionados en los anexos I y II de la Directiva (UE) 2022/2555. Además, esa estrategia debe conllevar un marco de gobernanza para alcanzar esos objetivos y prioridades, incluidas las políticas a que se refiere el artículo 7, apartado 2, de la Directiva (UE) 2022/2555.

31. Además, el artículo 7, apartado 1, letra c), de la Directiva (UE) 2022/2555 establece que la estrategia nacional de ciberseguridad debe incluir un marco de gobernanza que aclare las funciones y responsabilidades de las partes interesadas pertinentes a nivel nacional, que sustente la cooperación y la coordinación a nivel nacional entre las autoridades competentes, los puntos de contacto únicos y los CSIRT en virtud de la Directiva (UE) 2022/2555, así como la coordinación y la cooperación entre dichos organismos y las autoridades competentes con arreglo a actos jurídicos sectoriales de la Unión.

32. Por lo tanto, el requisito de adoptar una estrategia de ciberseguridad con arreglo al artículo 7 de la Directiva (UE) 2022/2555 no afecta a los requisitos de ciberseguridad impuestos a las entidades esenciales e importantes con arreglo a los artículos 21 y 23 de dicha Directiva, ni a las disposiciones relativas a su supervisión y aplicación establecidas en el capítulo VII, tal como exige el artículo 4, apartados 1 y 2, de la Directiva. La disposición pertinente del artículo 7 debe seguir siendo aplicable con respecto a los sectores, subsectores y tipos de entidades para los que existan actos jurídicos sectoriales específicos de la Unión en el sentido del artículo 4 de la Directiva (UE) 2022/2555.

III.3. **Designación de los CSIRT**

33. De conformidad con el artículo 10, apartado 1, de la Directiva (UE) 2022/2555, los Estados miembros deben designar o crear uno o varios CSIRT que cubran al menos los sectores, subsectores y tipos de entidades contemplados en los anexos I y II de la Directiva, incluidos, por tanto, los sectores, subsectores y tipos de entidades para los que existen actos jurídicos sectoriales específicos de la Unión. Normalmente, los CSIRT también llevarán a cabo sus tareas según lo establecido en el artículo 11, apartado 3, de la Directiva (UE) 2022/2555 a este respecto, a menos que se especifiquen tareas concretas en los actos jurídicos sectoriales específicos de la Unión.

III.4. **Marcos nacionales de gestión de crisis de ciberseguridad y EU-CyCLONe**

34. De conformidad con el artículo 9, apartado 1, de la Directiva (UE) 2022/2555, los Estados miembros deben designar o establecer una o varias autoridades de gestión de crisis cibernéticas que sean responsables de la gestión de incidentes y crisis de ciberseguridad a gran escala. Según el artículo 6, punto 7, de dicha Directiva, por incidente de ciberseguridad 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. El apartado 4 del artículo 9 de la Directiva (UE) 2022/2555 exige a los Estados miembros que adopten además un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se fijen los objetivos y las disposiciones de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. Este plan debe establecer, entre otros, los procedimientos de gestión de crisis de ciberseguridad, incluida su integración en el marco nacional general de gestión de crisis, y los canales para el intercambio de información, así como las partes interesadas y las infraestructuras públicas y privadas implicadas. Dichos procedimientos de gestión de crisis cibernéticas y las partes interesadas e infraestructuras públicas y privadas pertinentes podrían implicar procedimientos y partes interesadas específicos de cada sector.

35. El artículo 16 de la Directiva (UE) 2022/2555 establece la red de organizaciones de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe), cuyo objetivo es 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 relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión.

36. Dado que el artículo 9, relativo a los marcos de gestión de cibercrisis, y el artículo 16, relativo a EU-CyCLONe, no se refieren a los requisitos de ciberseguridad impuestos a las entidades en virtud de los artículos 21 y 23 de la Directiva (UE) 2022/2555 ni a la supervisión y ejecución establecidas en el capítulo VII, tal como exige el artículo 4, apartados 1 y 2, de dicha Directiva, los artículos 9 y 16 deben aplicarse en su totalidad a los sectores, a pesar de la existencia de actos jurídicos sectoriales específicos de la Unión a los que se refiere el artículo 4. En consecuencia, los Estados miembros deben designar o establecer una o varias autoridades competentes responsables de la gestión de incidentes y crisis de ciberseguridad a gran escala que se produzcan en los sectores cubiertos por actos jurídicos sectoriales de la Unión. Además, al adoptar el plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala no deben ignorarse los sectores cubiertos por actos jurídicos sectoriales específicos de la Unión. Por último, EU-CyCLONe debe llevar a cabo sus tareas consagradas en el artículo 16 de la Directiva (UE) 2022/2555 con respecto a los sectores en los que las entidades están sujetas a actos jurídicos sectoriales específicos de la Unión.

III.5. **Exclusión de la aplicación de los apartados 3 y 4 del artículo 3, del artículo 20 y de los apartados 2 y 3 del artículo 27**

37. De conformidad con el apartado 3 del artículo 3 de la Directiva (UE) 2022/2555, los Estados miembros deben elaborar una lista de las entidades esenciales e importantes, así como de entidades que presten servicios de registro de nombres de dominio que entren en el ámbito de aplicación de la Directiva. De conformidad con el apartado 2 del artículo 27, los Estados miembros exigirán a las entidades contempladas en el apartado 1 del artículo 27 de dicha Directiva que presenten determinada información a las autoridades competentes. Dado que el objetivo de estas disposiciones es garantizar una visión clara de las entidades incluidas en el ámbito de aplicación de la Directiva (UE) 2022/2555 para apoyar la supervisión de las entidades esenciales e importantes incluidas en su ámbito de aplicación, se deduce que estas disposiciones no deben aplicarse a las entidades a las que se aplique un acto jurídico sectorial específico de la Unión con respecto a los requisitos de información y gestión de riesgos en materia de ciberseguridad. Esto no impide que los Estados miembros incluyan dichas entidades en la lista.

De conformidad con el artículo 20, apartado 1, de la Directiva (UE) 2022/2555, los órganos de dirección de las entidades esenciales e importantes deben aprobar las medidas de riesgo en materia de ciberseguridad adoptadas por dichas entidades para dar cumplimiento a lo dispuesto en el artículo 21, supervisar su aplicación y pueden ser considerados responsables de las infracciones de dicho artículo por parte de las entidades. De conformidad con el artículo 20, apartado 2, de dicha Directiva, los Estados miembros velarán por que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a las entidades esenciales e importantes a ofrecer periódicamente a sus empleados una formación similar, al objeto de que adquieran los conocimientos y las competencias suficientes que les permitan identificar los riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad. Dado que las obligaciones derivadas del artículo 20 de la Directiva (UE) 2022/2555 están intrínsecamente vinculadas a los requisitos del artículo 21 de dicha Directiva, se deduce que el artículo 20 no debe aplicarse en el caso de actos jurídicos sectoriales específicos de la Unión en el sentido del artículo 4 de dicha Directiva que se apliquen con respecto a los requisitos de gestión de riesgos en materia de ciberseguridad.

APÉNDICE

Actos jurídicos sectoriales de la Unión

Reglamento (UE) 2022/2554 (Reglamento sobre la resiliencia operativa digital del sector financiero) ([1])

1. El artículo 1, apartado 2, del Reglamento (UE) 2022/2554 (Reglamento sobre la resiliencia operativa digital del sector financiero) establece que, en relación con las entidades financieras cubiertas por la Directiva (UE) 2022/2555 y sus correspondientes normas nacionales de transposición, el Reglamento (UE) 2022/2554 se considerará un acto jurídico sectorial de la Unión a efectos del artículo 4 de la Directiva (UE) 2022/2555. Esta afirmación se refleja en el considerando 28 del preámbulo de la Directiva (UE) 2022/2555, según el cual el Reglamento sobre la resiliencia operativa digital del sector financiero debe considerarse un acto jurídico sectorial específico de la Unión en relación con la Directiva (UE) 2022/2555 en lo que respecta a las entidades financieras. En consecuencia, se aplicarán las disposiciones del Reglamento (UE) 2022/2554 relativas a la gestión de riesgos de las tecnologías de la información y la comunicación (TIC) (artículo 6 y ss.), la gestión de incidentes relacionados con las TIC y, en particular, la notificación de incidentes graves relacionados con las TIC (artículo 17 y ss.), así como sobre las pruebas de resistencia operativa digital, (artículo 24 y ss.) los acuerdos de intercambio de información (artículo 25) y el riesgo de las TIC frente a terceros (artículo 28 y ss.), en lugar de las previstas en la Directiva (UE) 2022/2555. Por lo tanto, los Estados miembros no deben aplicar a ninguna entidad financiera comprendida en el Reglamento (UE) 2022/2554 las disposiciones de la Directiva (UE) 2022/2555 sobre gestión de riesgos de ciberseguridad y obligaciones de información, supervisión y ejecución.

2. A este respecto, se consideran entidades financieras las entidades a las que se refieren las letras a) a t) del apartado 1 del artículo 2 del Reglamento (UE) 2022/2554. Los tipos de entidades que entran en el ámbito de aplicación del Reglamento (UE) 2022/2554 como entidades financieras, así como en el ámbito de aplicación de la Directiva (UE) 2022/2555 como entidades esenciales o importantes, incluyen las entidades de crédito, los centros de negociación y las entidades de contrapartida central. Dado que es importante mantener una relación sólida y el intercambio de información con el sector financiero al amparo de la Directiva (UE) 2022/2555, las autoridades europeas de supervisión y las autoridades competentes en virtud del Reglamento (UE) 2022/2554 podrán solicitar participar en las actividades del Grupo de cooperación ([2]), e intercambiar información y cooperar con los puntos de contacto únicos, así como con los CSIRT y las autoridades competentes en virtud de la Directiva (UE) 2022/2555 ([3]). Las autoridades competentes a efectos del Reglamento (UE) 2022/2554 también deben transmitir información detallada sobre los incidentes graves relacionados con las TIC y, en su caso, sobre las ciberamenazas significativas, a los CSIRT, las autoridades competentes o los puntos de contacto únicos designados en virtud de la Directiva (UE) 2022/2555. Esto se puede conseguir facilitando el acceso inmediato a las notificaciones de incidentes y transmitiéndolas bien de forma directa, bien a través de un punto de entrada único. Los CSIRT deben estar en condiciones de ocuparse del sector financiero en sus actividades ([4]). Los Estados miembros deben seguir incluyendo al sector financiero en sus estrategias de ciberseguridad. Las disposiciones sobre los marcos nacionales de gestión de crisis cibernéticas [artículo 9 de la Directiva (UE) 2022/2555], así como sobre EU-CyCLONe [artículo 16 de la Directiva (UE) 2022/2555], deben seguir aplicándose a las entidades incluidas en el ámbito de aplicación del Reglamento (UE) 2022/2554.

([1]) Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333 de 27.12.2022, p. 1).

([2]) Artículo 14, apartado 3, de la Directiva (UE) 2022/2555 y artículo 47, apartado 1, del Reglamento (CE) 2022/2554.

([3]) Véase el considerando 28 de la Directiva (UE) 2022/2555.

([4]) Ibid.