CAPÍTULO II

La normativa y organización europea sobre ciberseguridad

Manfredi Matassa
Investigador postdoctoral en Derecho Administrativo de la Facultad de Derecho. Universidad de los Estudios de Palermo

SUMARIO. 1. Introducción. 2. El marco europeo de ciberseguridad. 2.1. La Directiva NIS2. *2.1.1. Las entidades incluidas. 2.1.2. Las obligaciones*. 2.2. El Reglamento DORA y la Directiva CER. **3. La organización europea de ciberseguridad.** 3.1. La Agencia de la Unión Europea para la Ciberseguridad (ENISA). 3.2. Los centros europeos de seguimiento y gestión de crisis cibernéticas. **4. El marco europeo de certificación de la ciberseguridad. 5. Conclusiones. 6. Bibliografía.**

1. Introducción

La ciberseguridad puede considerarse hoy en día una cuestión a la que los Estados deben enfrentarse necesariamente para salvaguardar el funcionamiento y el acceso de sus ciudadanos a los servicios esenciales, así como el buen funcionamiento de los procesos decisorios indispensables para la vida de cualquier democracia. El rápido desarrollo de las tecnologías del Internet de las Cosas (IoT)[1] parece estar conduciendo la red hacia

1. El concepto de IoT fue empleado por primera vez por el ingeniero británico Kevin Ashton para describir un sistema en el que los objetos del mundo físico pueden conectarse a la red mediante sensores. Los ejemplos de tecnologías IoT son ahora innumerables y están muy extendidos, como los coches, los hogares equipados con sistemas de domótica o las ciudades

un "punto de no retorno" (Denardis, 2020: 8) en el que internet está destinada a conectar ya no a individuos, sino principalmente a objetos. La difusión generalizada de estas tecnologías no solo ha exigido un replanteamiento radical de las formas de coexistencia de los ciudadanos con un nuevo "mundo de tecnologías de alto riesgo" (Perrow, 1984: 3), sino que también ha puesto en tela de juicio la frontera entre la realidad material y la dimensión virtual (en favor de una nueva perspectiva destinada a describir un mundo enteramente "on-life" [Floridi, 2015]). En tal escenario, la ciberseguridad merece contarse entre las cuestiones consideradas indispensables para el futuro de la Unión Europea, así como de cualquier organización compleja.

La Unión Europea no fue una de las primeras instituciones en adquirir plena conciencia de la necesidad de adoptar rápidamente modelos regulatorios capaces de abordar mejor los futuros desafíos de la ciberseguridad. Sin embargo, aunque esta última no ha surgido como un componente esencial del desarrollo y la seguridad europea hasta hace pocos años, hoy no sorprende la presencia de nada menos que once Estados europeos entre los veinte primeros puestos del Índice Global de Ciberseguridad (International Telecomunication Union, 2020: 25). De hecho, sin desmerecer en absoluto los esfuerzos individuales realizados por los Estados tradicionalmente más concienciados con la ciberseguridad (entre los que España[2] está en el podio, junto con Estonia y Lituania), hay que reconocer a la Unión Europea el papel de líder en la realización de una infraestructura de ciberseguridad de vanguardia.

El proceso que condujo a la creación de la actual arquitectura europea de defensa distó mucho de ser lineal. A lo largo de la última década, el legislador de la UE ha tenido que desempeñar un papel de coordinación entre numerosos actores que operan a distintos niveles para hacer frente a las diferentes necesidades —y, sobre todo, recursos disponibles— de los Estados miembros. Incluso hoy, en presencia de una noción de ciberseguridad en abstracto compartida por todos los países de la UE[3], el concepto en cuestión sigue siendo extremamente cambiante en función del ámbi-

inteligentes (según estimaciones recientes de la UE, este año podrían contarse 22 300 millones de dispositivos IoT conectados a la red).

2. Para un estudio sobre el estado de la ciberseguridad en España desde distintas perspectivas, véanse —entre los más recientes— Fuertes (2022); Fernández García (2022); Ballestero (2022).

3. Art. 2, apdo. 1, Reg. (UE) 2019/881: "[A los efectos del presente Reglamento, se entenderá por] 'ciberseguridad': todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

to de regulación de que se trate y de los diferentes objectivos perseguidos por los mismos.

Aunque los esfuerzos más recientes del legislador supranacional se han encaminado a construir una infraestructura de ciberseguridad autónoma y transversal a sus componentes individuales, el marco europeo de ciberseguridad sigue siendo un sistema extremadamente complejo que requiere un estudio en profundidad para ser comprendido en sus mecanismos más básicos. De hecho, hoy como ayer el funcionamiento eficaz de un sistema de este tipo requiere una aplicación tanto horizontal (cada ámbito de regulación debe combinarse con los demás) como vertical (en función del papel indispensable confiado a los Estados miembros para el funcionamiento de la arquitectura) (Wessel, 2015: 405).

Con dicho telón de fondo, este capítulo pretende recorrer la evolución normativa de la disciplina europea de la ciberseguridad, con la intención de poner de relieve la progresiva relevancia adquirida por el tema desde la segunda mitad de la pasada década. En particular, al ofrecer un análisis de las principales intervenciones europeas realizadas en la materia (con especial referencia a la Directiva NIS), así como de la actual organización europea de ciberseguridad, el estudio pretende ofrecer una visión general del estado de la cuestión y de las perspectivas de futuro de la ciberseguridad europea.

2. El marco europeo de ciberseguridad

La ciberseguridad ya figuraba entre las “cuestiones importantes” en una comunicación de la Comisión al Consejo y al Parlamento Europeo del año 2000 (Comisión de las Comunidades Europeas, 2000: 5). Sin embargo, a pesar de la creación en 2004 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés), una agencia con un mandato temporal situada en Heraclión (Grecia), y de otras acciones no especialmente incisivas (entre otras, véanse Comisión de las Comunidades Europeas, 2001, 2006, 2009), el tema no fue objeto de ninguna iniciativa relevante hasta la adopción de la estrategia europea de ciberseguridad en 2013 (Comisión Europea, 2013).

En este primer documento estratégico, la Unión Europea demostró cierta conciencia de la relevancia de la ciberseguridad en el futuro inmediato. En particular, tras destacar la conexión entre el funcionamiento de las tecnologías TIC, la resiliencia de las economías de los países miembros y la preservación de los derechos fundamentales de los ciudadanos,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

la estrategia establecía algunas de las prioridades cuya consecución se consideraba indispensable ante los próximos retos en materia de ciberseguridad (sobre todo, la conquista de la "ciberresiliencia" y el desarrollo de recursos industriales y tecnológicos en este ámbito). La publicación de este documento dio un impulso significativo a la inminente adopción del primer pilar normativo europeo sobre ciberseguridad, la Directiva (UE) 2016/1146, conocida como "Directiva NIS" (siglas en inglés de "redes y sistemas de información")[4]. Aunque con las limitaciones que se pondrán de manifiesto en el siguiente apartado, a esta directiva hay que reconocerle el mérito de haber identificado unos requisitos mínimos comunes en materia de ciberseguridad, de haber diseñado una primera infraestructura de coordinación entre la Unión Europea y los Estados miembros dentro de un mismo marco, y de haber reforzado los mecanismos de cooperación de la UE mediante la introducción de una red de Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés)[5].

Sin embargo, los cuantiosos daños causados por algunos ciberataques llevados a cabo tras la entrada en vigor de la Directiva NIS[6] pronto dejaron claro, en palabras del entonces presidente de la Comisión de la UE, que "los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques" (Juncker, 2017). La Unión Europea reaccionó a estos acontecimientos por una doble vía. En el plano estratégico, las instituciones europeas publicaron rápidamente una nueva versión actualizada de la estrategia europea de ciberseguridad, diseñada en torno a tres ejes: resiliencia, disuasión y defensa

4. 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.

5. Otro término utilizado con frecuencia para referirse a la red CSIRT es CERT-EU. Como señala Serini (2020: 251, n. 37): "Este acrónimo [CSIRT] se utiliza a menudo en lugar de otro acrónimo, CERT, es decir, *Computer Emergency Response Team*, que desempeña las mismas funciones que CSIRT. En realidad, la distinción entre ambos se debe a una mera cuestión de derecho de marcas, ya que CERT se creó por iniciativa de la agencia estadounidense DARPA [...], que creó el grupo en la Universidad Carnegie Mellon de Pittsburgh (Pensilvania), que sigue siendo propietaria de la marca en la actualidad. Por lo tanto, la distinción entre las dos siglas es que el uso de la denominación CSIRT está libre de cualquier obligación de marca registrada y, por lo tanto, no requiere el permiso de la Universidad Carnegie Mellon para su uso" (traducción del autor).

6. Pensemos, por ejemplo, en el ataque conocido como *WannaCry* —también llamado "el *ransomware* que cambió el mundo"—, que en 2017 logró infectar en poco tiempo más de 200 000 dispositivos en al menos setenta y cuatro países, cifrando la información contenida en los equipos atacados —muchos de ellos pertenecientes a infraestructuras hospitalarias— y exigiendo alrededor de 300 dólares en bitcoines por cada dispositivo afectado para descifrar los datos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

frente a los ciberataques (Comisión Europea, 2017). Paralelamente, en la vertiente normativa, las mismas instituciones han comenzado a buscar un entendimiento sobre el contenido del futuro Reglamento (UE) 2019/881[7], con el que la UE ha rediseñado gran parte de la infraestructura europea de defensa de la ciberseguridad (que se tratará con más detalle en las páginas siguientes).

El plan estratégico de ciberseguridad de la Unión se actualizó por última vez en 2020, cuando se publicó la Estrategia de la UE para la Década Digital (Comisión Europea, 2020), con el objetivo principal de institucionalizar en el contexto europeo los distintos principios de ciberseguridad surgidos en el "Paris Call for Trust and Security in Cyberspace" de 2018[8]. La nueva estrategia ha puesto de relieve algunas cuestiones específicas, sin desviarse del camino ya trazado por el anterior documento de 2017. Sin embargo, en el documento más reciente, la Unión hizo hincapié en la importancia de ir más allá del enfoque anterior esbozado en la Directiva NIS, mediante la adopción de un nuevo texto elaborado a partir de un concepto integral de ciberresiliencia. En términos más generales, la última estrategia hace hincapié en la necesidad de iniciar una segunda fase de políticas de ciberseguridad mucho más ambiciosa que la anterior, que se materializa mediante la adopción de un paquete legislativo compuesto por tres elementos fundamentales: el Reglamento (UE) 2022/2554 (Reglamento DORA)[9] y las directivas (UE) 2022/2555 (Directiva NIS2)[10] y 2022/2557 (Directiva CER)[11]. El contenido de estas tres intervenciones merece un análisis aparte.

7. 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).

8. La "Paris Call" de 2018 fue una iniciativa en la que participaron unos ochenta países de todo el mundo, junto con empresas y organizaciones internacionales líderes que operan en el sector de la tecnología y la ciberseguridad, con el objetivo de desarrollar una estrategia de acción colectiva para mejorar la confianza, la seguridad y la estabilidad en el ciberespacio. El acuerdo final fue firmado por unos cincuenta países —aunque no por aquellos con mayor potencial ciberofensivo, como China, Rusia, Irán y Corea del Norte—, ciento treinta empresas y otras ochenta organizaciones, entre ellas varias universidades de prestigio de todo el mundo.

9. Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.

10. 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.

11. Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

2.1. La Directiva NIS2

La Directiva NIS2 se introdujo para subsanar algunas limitaciones evidentes del texto anterior, y es el pilar fundamental de la actual infraestructura europea de ciberseguridad.

La primera Directiva NIS había elaborado criterios comunes de identificación destinados a determinar un núcleo mínimo e indispensable de protección para determinados sujetos, operadores de servicios esenciales (OSE) y proveedores de servicios digitales (PSD), con el fin de poder garantizar la continuidad de los servicios esenciales a escala europea. Sin embargo, ya en los primeros años de vida de la Directiva, se comprobó que los parámetros para determinar su ámbito de aplicación objetivo eran inadecuados para garantizar un grado adecuado de protección de la seguridad y los intereses europeos. De hecho, al observar los sectores descritos analíticamente en el Anexo II, se aprecia que la primera directiva europea de ciberseguridad había excluido de su ámbito de aplicación, entre otros, el sector alimentario, el espacial, el químico, el nuclear y, sobre todo, toda la Administración pública.

La nueva Directiva NIS2, que entró en vigor el 17 de enero de 2023, mantiene el mismo espíritu que la normativa anterior, pero eleva significativamente el nivel de seguridad de las redes europeas, empezando precisamente por la asignación de nuevos criterios para la identificación de las que deben protegerse.

En concreto, el texto de 2022 pretendía colmar la laguna anteriormente descrita avanzando en dos direcciones. Por un lado, la Directiva ha ampliado las obligaciones de ciberseguridad a una amplia gama de operadores de servicios públicos y privados esenciales que anteriormente no estaban incluidos en el ámbito de aplicación de la NIS (no solo las Administraciones públicas, sino también las entidades que operan en los sectores de la producción de dispositivos médicos, la ingeniería aeroespacial, la gestión de residuos, la producción de alimentos y los servicios postales). Por otro lado, ha formulado criterios de autoaplicación más precisos y uniformes, con la intención de reducir las diferencias entre los niveles de ciberseguridad ofrecidos por los Estados miembros.

2.1.1. Las entidades incluidas

En referencia al primer perfil, el apdo. 1 del art. 1 de la Directiva NIS2 estipula que es aplicable a todas las entidades públicas y privadas que se consideren

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

"medianas empresas" en el sentido del art. 2, apdo. 1, del anexo de la Recomendación 2003/361/CE[12], y cuyos servicios o actividades se lleven a cabo dentro de la Unión y entren dentro de los sectores estratégicos identificados en las directivas. La distinción más obvia se remonta a la decisión de abandonar la categorización elaborada por la anterior directiva NIS entre OSE y PSD, en favor de una distinción sin precedentes entre "entidades esenciales" y "entidades importantes". Las "entidades esenciales" se identificaron como aquellos actores cuya interrupción del servicio tendría un impacto directo e inmediato en el funcionamiento de la sociedad y la economía (por ejemplo, las empresas públicas o privadas que operan en los sectores de la energía, el transporte sanitario y el suministro central, pero también todas las Administraciones centrales de los países miembros)[13]. Las "entidades importantes", aunque no críticas en la misma medida que las primeras, se han identificado como aquellas entidades con funciones significativas dentro de la economía digital y social (incluidos servicios digitales como motores de búsqueda, computación en la nube y plataformas en línea)[14].

Otra novedad importante introducida por la NIS2 es la incorporación de una disciplina específica para regular su ámbito de aplicación con respecto a las entidades públicas. De hecho, partiendo del supuesto de que uno de los límites más evidentes de la disciplina anterior estaba relacionado precisamente con la ausencia de cualquier referencia a las Administraciones públicas, la nueva formulación de la Directiva pretendía especificar qué Administraciones quedaban automáticamente implicadas en el ámbito de aplicación de la Directiva, y cuáles, en cambio, quedaban sujetas a las prescripciones de la NIS2 sobre la base de las indicaciones expresadas por cada uno de los Estados miembros.

La primera categoría examinada incluye todas las Administraciones centrales de los países de la UE identificadas según los parámetros de la legislación nacional[15]. Sin embargo, aprovechando, asimismo, las leccio-

12. Art. 2, apdo. 1, Anexo de la Rec. 2003/361/CE: "La categoría de microempresas, pequeñas y medianas empresas (PYME) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros". Conviene precisar que el apdo. 1 del art. 2 de la Directiva NIS2 tiene por objeto dejar sin efecto, a los fines de aplicación de dicha directiva, el apdo. 4 del art. 3 del mismo anexo, en la medida en que este disponía: "A excepción de los casos citados en el segundo párrafo del apartado 2, una empresa no puede ser considerada como PYME si el 25 % o más de su capital o de sus derechos de voto están controlados, directa o indirectamente, por uno o más organismos públicos o colectividades públicas".
13. Art. 3, apdo. 1, Dir (UE) 2022/2555.
14. Art. 3, apdo. 2, Dir. (UE) 2022/2555.
15. Art. 2, apdo. 2, letra i), Dir. (UE) 2022/2555.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

nes del pasado, el legislador europeo de 2022 también adoptó una posición explícita con respecto a la importancia de las entidades de ámbito regional. No obstante, se consideró que estas últimas estaban sujetas a las obligaciones impuestas por la Directiva NIS2 no tanto sobre la base de un mecanismo de autoaplicación, sino tras una "evaluación [del Estado miembro] basada en el riesgo"[16], según la cual la interrupción de la prestación de un servicio "podría tener un impacto significativo en actividades sociales o económicas críticas"[17]. Por otra parte, en referencia a la participación de entidades públicas de menor tamaño, la NIS2 preveía —aunque sin aportar criterios precisos— la posibilidad de que los Estados miembros ampliaran el régimen de aplicación a los organismos de las Administraciones locales y a los centros de enseñanza (en particular, cuando realizaran actividades de investigación en ámbitos considerados críticos).

Sobre la base de lo que se ha destacado hasta ahora, se observa que, gracias sobre todo a un buen equilibrio entre los criterios de autoaplicación y la aplicación en los Estados miembros, el cambio de enfoque del legislador europeo ha permitido una ampliación significativa y claramente visible de las materias implicadas dentro de la disciplina. No obstante, para comprender el alcance real de la Directiva NIS II, será necesario esperar a la plena aplicación de algunas medidas, ya que, en cualquier caso, corresponderá a los Estados miembros definir, a más tardar el 17 de abril de 2025, una lista de actores esenciales e importantes que deberán facilitar la información necesaria.

A lo anterior hay que añadir que los Estados miembros tienen la posibilidad de establecer medidas para modificar en sentido restrictivo el contenido de los criterios de autoaplicación identificados directamente por la Unión, de conformidad con la "prerrogativa estatal" en materia de seguridad nacional reconocida a los Estados miembros[18]. En efecto, dado que —como se verá más adelante— el cumplimiento de las medidas contenidas en la Directiva podría dar lugar a la difusión de información atribuible a la defensa y a la seguridad nacional, el legislador europeo ha incluido dentro de la NIS2 un conjunto de normas destinadas a delimitar el

16. El apdo. 9 del art. 6 de la Dir. (UE) 2022/2555 define el "riesgo" como "la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente".

17. Art. 2, apdo. 2, letra ii), Dir. (UE) 2022/2555.

18 Se hace referencia al apdo. 2 del art. 4 del Tratado de la Unión Europea (TUE), en la medida en que establece que "respetará las funciones esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ámbito de aplicación de la Directiva de conformidad con el citado apdo. 2 del art. 4 TUE[19]. Por lo tanto, el alcance real de esta directiva solo puede depender del grado de penetración que el concepto de seguridad nacional asuma cuando se aplique en los distintos Estados miembros.

2.1.2. Las obligaciones

Como ya se ha mencionado, además de la significativa ampliación del ámbito subjetivo, uno de los principales méritos de la Directiva 2022/2555 es la detallada previsión de los cumplimientos encomendados a los Estados miembros, así como las obligaciones conexas de las entidades públicas y privadas incluidas. Entre ellas, se considera oportuno ofrecer una visión general de (*i*) las medidas de gestión de riesgos de ciberseguridad, (*ii*) las obligaciones de información, (*iii*) las medidas de supervisión y ejecución, y (*iv*) la regulación de las multas administrativas dirigidas a las entidades "esenciales" e "importantes".

El legislador europeo ha definido las medidas de gestión de riesgos de ciberseguridad a través de directrices precisas. En particular, la Directiva NIS2 se ocupa de indicar a los Estados miembros los parámetros que deben utilizarse tanto para orientar la actuación administrativa de los Estados hacia los cánones de proporcionalidad como en relación con la evaluación de los ciberriesgos[20]. Por lo que se refiere al primer aspecto, el legislador europeo ha precisado determinados factores que deben tenerse en cuenta a la hora de aplicar medidas de gestión. En este sentido, además de prestar especial atención a los costes de aplicación de estas medidas, el artículo 21 establece que los instrumentos a disposición de los Estados miembros deben emplearse teniendo en cuenta el nivel de seguridad de los ordenadores y de las redes en función de los riesgos existentes (y no, por tanto, solo potenciales). Sobre esta base, pues, la misma disposición indica los criterios que deben utilizarse para evaluar la proporcionalidad de tales medidas, a saber: (*i*) el grado de exposición del sujeto a los riesgos, (*ii*) el tamaño del sujeto, (*iii*) la probabilidad de que se produzcan incidentes, y (*iv*) su gravedad, incluidas sus repercusiones sociales y económicas. En relación con el segundo aspecto, el legislador europeo ha insistido en la necesidad de adoptar un "enfoque multirriesgo" basado en determinadas

19. Así, de conformidad con el apdo. 7 del art. 2 de la Dir. (UE) 2022/2555, quedan excluidas del ámbito de aplicación de la Directiva "[...] las entidades de la Administración pública que lleven a cabo sus actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley, incluidas la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales".

20. Art. 21, apdo. 1, Dir. (UE) 2022/2555.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

medidas bien definidas y recogidas en una lista[21]. Entre ellas cabe mencionar, sin ninguna pretensión de exhaustividad, la especial atención prestada a la gestión de las copias de seguridad (*backup*) y la restauración de los sistemas en caso de catástrofe, la seguridad de los sistemas de contratación (*supply chains*), así como la protección de las prácticas básicas de "higiene informática" y la formación en ciberseguridad.

La articulación normativa de la NIS2 es especialmente puntual en lo que respecta a la regulación de las obligaciones de información. Adoptando un enfoque pragmático, el legislador europeo ha esbozado un sistema que impone a los agentes esenciales e importantes la obligación de notificar sin demora a las autoridades competentes o a los CSIRT (véase *infra*) cualquier incidente de seguridad "que tenga un impacto significativo". Por lo que aquí interesa, parece oportuno adentrarse en la definición que el legislador europeo ofrece del concepto de "incidente significativo" para, a continuación, concretar las obligaciones de información que incumben a las partes incluidas en el ámbito de aplicación de la NIS2.

La noción de "incidente significativo" adquiere relevancia en primer lugar dentro de la infraestructura europea de ciberseguridad con vistas a completar el esfuerzo de definición realizado por el legislador europeo en la primera parte de la Directiva en referencia a los conceptos de "ciberamenaza"[22], "cuasiincidente"[23], "incidente"[24] e "incidente de ciberseguridad a gran escala"[25]. Sin embargo, para garantizar una mayor uniformidad de la disciplina en todo el territorio europeo, el legislador de la NIS2 ha concretado este concepto de una manera menos abstracta que los anteriores —superando así una de las limitaciones de la primera Di-

21. Para un análisis más detallado de las medidas individuales, consúltese el contenido del apdo. 1 del art. 21 de la Dir. (UE) 2022/2555.

22. En relación con la noción de "ciberamenaza", el art. 6.1 establece una referencia cruzada a la definición del art. 2, apdo. 8, del Reg. (UE) 2019: "cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas".

23. Art. 6, apdo. 5, Dir. (UE) 2022/2555: "'cuasiincidente': un hecho que habría podido comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos, pero cuya materialización completa se previno de manera satisfactoria o que no llegó a materializarse".

24. Art. 6, apdo. 6, Dir. (UE) 2022/2555: "'incidente': todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos".

25. Art. 6, apdo. 7, Dir. (UE) 2022/2555: "'incidente de ciberseguridad a gran escala': 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".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

rectiva NIS—, identificando dos características. En concreto, con arreglo al apdo. 3 del art. 23 de la Directiva 2022/2555, un incidente puede considerarse "significativo" si (*i*) "ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada", o (*ii*) "puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables"[26].

Tras desarrollar este concepto, el legislador europeo vinculó la ocurrencia de un accidente significativo a determinadas obligaciones precisas de notificación. En un primer informe, definido de "alerta temprana", los implicados están obligados a indicar, en un plazo de 24 horas desde que tienen conocimiento del incidente, si se sospecha que este "responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas"[27]. En un informe posterior, que debe presentarse en las 48 horas siguientes, se pide a los destinatarios de la Directiva que actualicen la información anterior para poner de relieve —en la medida de lo posible— la gravedad, el impacto del incidente significativo y los eventuales indicadores de deterioro[28]. En un informe final más detallado, que deberá presentarse a los organismos competentes en el plazo de un mes a partir de la notificación del informe anterior, se pide esta vez a las entidades NIS2 que elaboren una descripción detallada del incidente, destinada a indicar el tipo de amenaza o la causa principal que probablemente lo desencadenó, las medidas paliativas adoptadas y en curso, así como el eventual impacto transfronterizo del mismo[29]. Además, el legislador europeo ha completado el marco reglamentario examinado con un sistema de notificación voluntaria válido en caso de que agentes esenciales e importantes[30], como también otras entidades no implicadas en la Directiva[31], se vean implicados en ciberamenazas, incidentes o cuasiincidentes.

Como ya se ha mencionado, entre los principales cumplimientos contenidos en la Directiva NIS2, merecen especial atención las medidas

26. Así pues, el concepto de "incidente significativo" del art. 23, apdo. 3, parece totalmente superponible al de "amenaza significativa" del art. 6, apdo. 11: "'ciberamenaza significativa': una ciberamenaza que, basándose en sus características técnicas, cabe suponer que tiene el potencial de provocar repercusiones graves en los sistemas de redes y de información de una entidad o para los usuarios de los servicios de la entidad causando perjuicios materiales o inmateriales considerables".

27. Art. 23, apdo. 4, letra a), Dir. (UE) 2022/2555.

28. Art. 23, apdo. 4, letra b), Dir. (UE) 2022/2555. Además, cabe señalar que la siguiente letra c) prevé un tercer informe, intermedio y solo eventual, obligatorio únicamente a petición de los CSIRT u otras autoridades consideradas competentes.

29. Art. 23, apdo. 4, letra d), Dir. (UE) 2022/2555.

30. Art. 30, apdo. 1, letra a), Dir. (UE) 2022/2555.

31. Art. 30, apdo. 1, letra b), Dir. (UE) 2022/2555.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de supervisión y ejecución de las entidades esenciales e importantes. La Directiva de 2022 atribuye en primer lugar a los Estados miembros la tarea de garantizar que las medidas de supervisión o ejecución impuestas a estos sujetos sean efectivas, proporcionadas y disuasorias (fórmula que, como veremos, también se propondrá más adelante en referencia al régimen sancionador)[32]. Tras consagrar este principio general, la Unión identifica un núcleo de competencias mínimas a disposición de los Estados mediante la elaboración de una lista de medidas de supervisión específicas que incluyen: (*i*) inspecciones *in situ* y supervisión a distancia, incluidos controles aleatorios; (*ii*) auditorías de seguridad periódicas y específicas llevadas a cabo por un organismo independiente o una autoridad competente, o auditorías *ad hoc*; (*iii*) solicitudes de informaciones necesarias para evaluar las medidas para la gestión de riesgos de ciberseguridad; y (*iv*) solicitud de acceso a datos, documentos y otras informaciones[33]. Por lo que se refiere en particular a las auditorías, debe concederse especial importancia al segundo párrafo del apartado 2 del artículo 32, en la parte en que, tras subrayar la necesidad de poner los resultados de dichas auditorías a disposición de la autoridad competente, la Directiva especifica que los costes de las auditorías de seguridad realizadas por organismos independientes correrán a cargo del sujeto de la auditoría (a menos que, debidamente justificado, la autoridad competente decida lo contrario)[34].

Tras haber indicado los poderes mínimos de supervisión, el legislador europeo proporcionó una lista igualmente puntual de los poderes mínimos de ejecución de las medidas NIS2 de los Estados miembros. Tras indicar los poderes mínimos de supervisión, el legislador europeo proporcionó una lista igualmente precisa de los poderes mínimos de ejecución de las medidas SRI por parte de los Estados miembros[35]. Entre ellas figura la posibilidad de que las autoridades designadas por ellos como competentes: (*i*) aperciban por incumplimientos de la misma NIS2 por parte de las entidades afectadas; (*ii*) exijan a los mismos que pongan fin a las conductas que infringen la Directiva y que se abstengan de repetirlas; (*iii*) ordenen a las entidades afectadas que apliquen las recomendaciones

32. Art. 32, apdo. 1, Dir. (UE) 2022/2555.
33. Art. 32, apdo. 2, Dir. (UE) 2022/2555.
34. La indicación de la asunción de costes por parte de las "entidades NIS" como norma general, con posibles excepciones debidamente justificadas, merece ser valorada en el marco de un contexto más amplio y complejo. En efecto, el funcionamiento actual de la infraestructura de ciberseguridad multinivel requiere un esfuerzo económico individual por parte de las pymes —no siempre fácilmente sostenible, especialmente para las pequeñas empresas—, recompensado con beneficios que se extienden en general a todo el sistema económico. Para un estudio reciente sobre este tema véase Kaiser (2023).
35. Art. 32, apdo. 4, Dir. (UE) 2022/2555.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

formuladas a raíz de una auditoría de seguridad en un plazo razonable; y (*iv*) impongan o soliciten la imposición, por parte de los organismos u órganos jurisdiccionales competentes de acuerdo con la legislación nacional, de una multa administrativa adicional respecto de cualquier medida prevista por el mismo artículo.

En caso de que las medidas de ejecución adoptadas respecto a "entidades esenciales" resulten ineficaces, la NIS2 exige a los Estados miembros que, en el respeto del principio de proporcionalidad, fijen 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[36]. En caso de que el destinatario no cumpla en ese plazo, la Directiva otorga a los Estados miembros poderes bastante amplios para hacer frente a cualquier incumplimiento por parte de los destinatarios de las medidas de ejecución NIS2. En efecto, estos últimos están obligados por la Directiva a otorgar a sus autoridades competentes poderes destinados tanto a afectar a la actividad del moroso como —y esto es menos obvio— a la esfera de las personas físicas con funciones ejecutivas. En particular, la Directiva 2022 prevé, por un lado, la necesidad de suspender temporalmente una certificación o autorización referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por la entidad esencial[37], y, por otro lado, permite (*rectius*, exige) a los Estados miembros introducir medidas capaces de prohibir temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial ejercer funciones de dirección en la misma[38].

Como ya se ha mencionado, el marco normativo descrito encuentra un cierre coherente con las disposiciones de la Directiva NIS2 sobre multas administrativas. Al igual que en el caso de las medidas de supervisión y ejecución, este marco fue concebido por el legislador europeo con la intención de introducir medidas efectivas, proporcionadas y disuasorias. Sin embargo, en comparación con las anteriores, las finalidades disuasorias son mucho más pronunciadas: en el caso de las "entidades esencia-

36. Art. 32, apdo. 5, Dir. (UE) 2022/2555. La exclusión de las "entidades importantes" de la disciplina en cuestión puede deducirse a contrario de la lectura del siguiente artículo 33.

37. Art. 32, apdo. 5, letra a), Dir. (UE) 2022/2555.

38. Art. 32, apdo. 5, letra b), Dir. (UE) 2022/2555. Las medidas excepcionales consideradas tienen carácter temporal y, por lo tanto, no se les puede atribuir un valor punitivo. Sin embargo, la evidente capacidad lesiva de estas medidas llevó al legislador europeo a condicionar su utilización al cumplimiento de las garantías procesales adecuadas para asegurar el recurso efectivo a las autoridades judiciales y un proceso justo, la presunción de inocencia y, más en general, los derechos de defensa de los destinatarios.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

les", el marco europeo prevé una sanción pecuniaria administrativa de un máximo de al menos diez millones de euros o de al menos el 2 % del volumen de negocios global anual total del ejercicio anterior (la cifra que sea más elevada)[39], mientras que en el caso de las "entidades importantes" los límites máximos descienden ligeramente (siete millones de euros o el 1,4 % del volumen de negocios global, respectivamente)[40]. Además, para imponer a un sujeto esencial o importante el cese de una infracción establecida por la Directiva y constatada por una decisión previa de la autoridad competente, la misma disposición permite a los Estados miembros la posibilidad de utilizar el instrumento de la multa coercitiva[41].

Por último, cabe señalar que el legislador europeo ha atribuido expresamente a las disposiciones sobre sanciones pecuniarias administrativas relacionadas con el incumplimiento de las obligaciones NIS2 un carácter autoejecutable[42]. Por lo tanto, incluso en caso de no aplicación de la Directiva antes del 17 de octubre de 2024, los Estados miembros podrán seguir haciendo uso del citado artículo a efectos de imponer sanciones efectivas, proporcionadas y disuasorias.

2.2. El Reglamento DORA y la Directiva CER

Tal como están las cosas, la Directiva NIS2 representa inequívocamente el corazón palpitante del marco normativo europeo en materia de ciberseguridad. Sin embargo, el marco normativo diseñado por la Directiva 2022/2555 está íntimamente entrelazado con otros dos textos aprobados al mismo tiempo que la NIS2, a saber, el Reglamento 2022/2554, conocido como DORA (*Digital Operational Resilience Act*)[43], y la Directiva 2022/2557, conocida como CER (*Critical Entity Resilience*)[44].

39. Art. 34, apdo. 4, Dir. (UE) 2022/2555.
40. Art. 34, apdo. 5, Dir. (UE) 2022/2555.
41. Art. 34, apdo. 6, Dir. (UE) 2022/2555.
42. Art. 34, apdo. 8, Dir. (UE) 2022/2555, según el cual: "Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, ese Estado miembro velará por que el presente artículo se aplique de tal modo que la incoación de la multa corresponda a la autoridad competente y su imposición, a los órganos jurisdiccionales nacionales competentes, garantizando al mismo tiempo que estas vías de acción sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades competentes".
43. Reg. (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.
44. Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

El Reglamento DORA se adoptó con el objetivo de introducir medidas *ad hoc* para garantizar un mayor nivel de ciberseguridad en el sector financiero de la UE. En particular, este reglamento se centra en reforzar la capacidad de las entidades financieras para prevenir, mitigar y responder eficazmente a los incidentes digitales, que podrían tener repercusiones significativas no solo a nivel corporativo, sino también en el sistema financiero europeo en general. La opción del legislador europeo de garantizar un nivel de ciberseguridad en el sector financiero superior al garantizado por las medidas NIS2 debe enmarcarse en un marco jurídico bien definido. El contenido del DORA debe evaluarse en el marco de los "actos jurídicos sectoriales de la Unión" regulados por el artículo 4 de la Directiva 2022/2555[45], de modo que las obligaciones previstas en el mismo solo se aplicarán en la medida en que sus efectos sean al menos equivalentes a los efectos mínimos previstos en la NIS2 (que serán de alcance residual en caso de lagunas en la regulación sectorial).

La Directiva 2022/2557, en cambio, debe enmarcarse en términos bastante diferentes a los de la normativa examinada hasta ahora. Esta directiva, a diferencia del DORA, no define específicamente el alcance de las medidas contenidas en el NIS2, pero introduce una disciplina transversal que permite ver cómo el concepto de "seguridad de las infraestructuras" trata los peligros del mundo real de la misma manera que los de la dimensión cibernética. Tanto es así que la Directiva CER debe considerarse en un contexto más amplio, el de la protección de las "infraestructuras críticas" indispensables para el mantenimiento de las funciones sociales y económicas esenciales para la vida de la Unión y para la seguridad de sus ciudadanos.

En concreto, la Directiva en cuestión pretendía introducir en el marco normativo europeo un concepto de seguridad capaz de integrar el componente físico con el cibernético (en la perspectiva ya descrita de una realidad *onlife*). En concreto, la identificación de los sujetos considerados críticos en el marco de la Directiva ERC reviste una importancia central también —y en nuestra perspectiva especialmente— para el buen funcionamiento de la Directiva NIS2[46]. Por un lado, contemplando esta rela-

45. Art. 1, apdo. 2, Reg. (UE) 2022/2554, según el cual: "En relación con las entidades financieras identificadas como entidades esenciales o importantes en virtud de las normas nacionales de transposición del artículo 3 de la Directiva (UE) 2022/2555, el presente Reglamento se considerará un acto jurídico sectorial de la Unión a efectos del artículo 4 de dicha Directiva".

46. En particular, el considerando 9 de la Directiva (UE) 2022/2557 establece: "Dada la importancia de la ciberseguridad para la resiliencia de las entidades críticas y en aras de la coherencia, debe garantizarse, siempre que sea posible, un enfoque coherente entre la presente Directiva y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ción desde la perspectiva de la ciberseguridad, la elaboración de un concepto común de "infraestructura crítica" se hace indispensable para la identificación del perímetro de aplicación del marco europeo en materia de ciberseguridad. De hecho, tras señalar que "las entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557, deben ser consideradas entidades esenciales a los efectos de la presente Directiva"[47], esta última señala que las mismas obligaciones debían aplicarse también a las entidades identificadas por la CER "independientemente de su tamaño"[48]. Por otra parte, desde la perspectiva de la seguridad de los componentes físicos, el legislador europeo pretendía extender un alto nivel de protección a los sujetos ya identificados por la NIS2 también en el frente de la seguridad "tradicional", mediante la introducción de medidas para hacer frente a los riesgos no informatizados.

3. La organización europea de ciberseguridad

El análisis de contenido previamente realizado de las fuentes europeas de ciberseguridad más relevantes quedaría incompleto sin una representación adecuada de la infraestructura organizativa europea de ciberseguridad diseñada por el Reglamento (UE) 2019/881. En este contexto, el siguiente análisis pretende investigar la configuración y el funcionamiento de los principales componentes de la infraestructura europea de ciberseguridad introducida por el *Cybersecurity Act,* prestando especial atención a (*i*) la estructura y las funciones de ENISA, (*ii*) al marco europeo de certificación de la ciberseguridad y, por último, (*iii*) a los mecanismos de gestión y respuesta a las crisis cibernéticas.

3.1. La Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Como ya se ha mencionado, ENISA fue concebida inicialmente por el Reglamento (CE) 2004/460 como una agencia temporal con funciones muy limitadas. Sin embargo, a medida que aumentaban los riesgos e intereses relacionados con la ciberseguridad, el legislador europeo amplió el man-

47. La cuestión se aborda en términos generales en el considerando 30 de la Directiva (UE) 2022/2555, según el cual: "En vista de las interrelaciones que existen entre la ciberseguridad y la seguridad física de las entidades, debe garantizarse un enfoque coherente entre la Directiva (UE) 2022/2557 [...] y la presente Directiva. Para ello, las entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557, deben ser consideradas entidades esenciales a los efectos de la presente Directiva".

48. Art. 2, apdo. 3, Dir. (UE) 2022/2555, según el cual: "Independientemente de su tamaño, la presente Directiva se aplica a las entidades que se identifiquen como entidades críticas con arreglo a la Directiva (UE) 2022/2557".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

dato de la Agencia en varias ocasiones[49], hasta darle un carácter permanente con motivo de la reorganización global de la arquitectura europea de ciberseguridad permitida por el Reglamento (UE) 2019/881.

El mandato y los objetivos de ENISA se establecen en el Capítulo I del Título II del primer reglamento europeo de ciberseguridad. A un nivel muy general, la Ley de Ciberseguridad encomienda a ENISA que logre un alto nivel común de ciberseguridad en la UE también apoyando activamente a los Estados miembros, instituciones, órganos, oficinas y agencias de la UE en la mejora de la ciberseguridad, así como que contribuya a reducir la fragmentación del mercado interior de la UE[50]. Los objetivos asignados a ENISA los lleva a cabo de manera independiente (especialmente frente a la Comisión) y teniendo debidamente en cuenta las actividades y competencias asignadas a los Estados miembros[51]. Entre las principales competencias que el Reglamento de 2019 confiere a la Agencia figuran las de: (*i*) aplicación de políticas y legislación a nivel europeo y desarrollo de las capacidades de ciberseguridad de los Estados miembros[52], (*ii*) apoyo a la cooperación operativa a nivel de la Unión[53] e internacional[54], (*iii*) desarrollo de políticas de la UE sobre certificación de productos TIC[55], y (*iv*) sensibilización del público sobre los riesgos de ciberseguridad[56].

Con especial referencia a las funciones de cooperación operativa, tema al que volveremos en la parte final del estudio, ENISA tiene encomendada la organización de ejercicios periódicos, así como, cuando lo soliciten, el apoyo a los Estados miembros, instituciones, organismos y agencias de la UE en la organización de ejercicios. Los primeros son ejercicios que se realizan periódicamente "a nivel de la Unión", con el objetivo de mejorar la cooperación entre los Estados miembros, las instituciones y otras partes interesadas, así como la respuesta colectiva a los incidentes cibernéticos. En concreto, se llevan a cabo mediante el diseño y la puesta a prueba de protocolos de comunicación, procedimientos de respuesta y otros mecanismos de colaboración vertical y horizontal. Estos últimos tie-

49. En particular, el plazo de cinco años del mandato de ENISA previsto inicialmente en el artículo 27 del Reg. (CE) 2004/460 fue prorrogado de forma continua por los posteriores reglamentos 2008/1997, 2011/580 y 2016/526.
50. Art. 3, apdo. 1, Reg. (UE) 2019/881.
51. Art. 3, apdo. 3, Reg. (UE) 2019/881.
52. Respectivamente, arts. 5 y 6 Reg. (UE) 2019/881.
53. Art. 7 Reg. (UE) 2019/881.
54. Art. 12 Reg. (UE) 2019/881.
55. Art. 8 Reg. (UE) 2019/881. Merece la pena especificar que el marco europeo de certificación de la ciberseguridad se rige por su propia disciplina dentro del Título III (artículos 46-65) del mismo reglamento, y será objeto de un debate autónomo más adelante.
56. Art. 10 Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

nen lugar a escala mundial y su participación es significativamente más amplia y compleja. Se trata de ejercicios diseñados cada dos años para simular escenarios de crisis cibernéticas a gran escala que requieren una intensa coordinación entre distintos niveles de gobierno y sectores. En este caso, el objetivo es poner a prueba y mejorar la capacidad de resistencia y respuesta de la Unión en su conjunto, al tiempo que se evalúa la eficacia de las medidas de seguridad aplicadas y se detectan posibles lagunas o puntos débiles en las estrategias de ciberseguridad[57].

Por lo demás, el *Cybersecurity Act* replanteó la estructura organizativa de ENISA prevista inicialmente en el Reglamento (CE) 2004/460, introduciendo una estructura administrativa y de gestión compuesta por (*i*) un consejo de administración, (*ii*) un comité ejecutivo, (*iii*) un director ejecutivo, (*iv*) un grupo consultivo, y (*v*) una red de funcionarios de enlace[58].

El Consejo de Administración está compuesto por un miembro nombrado por cada Estado miembro y dos miembros nombrados por la Comisión[59]. El Reglamento de 2019 dio más peso que en el marco anterior a las posiciones expresadas por los representantes de los Estados miembros[60]. De hecho, la "nueva" redacción no solo reduce a dos el número de miembros con derecho a voto nombrados por la Comisión (antes eran tres), sino que también elimina el comité del consejo sin derecho a voto formado por representantes de la industria, consumidores y expertos académicos en ciberseguridad. Más aún, a diferencia del esquema anterior, el *Cybersecurity Act* identifica las funciones desempeñadas por la junta a través de una lista analítica y bastante definida[61]. Entre estas últimas funciones, cabe destacar, sin ánimo de exhaustividad, las relacionadas con la adopción y supervisión

57. Art. 7, apdo. 5, Reg. (UE) 2019/881.
58. Art. 13 Reg. (UE) 2019/881.
59. Art. 14, apdo. 1, Reg. (UE) 2019/881. Además, según el siguiente apdo. 4: "El mandato de los miembros del Consejo de Administración y de sus suplentes será de cuatro años. Este mandato será renovable".
60. Según el marco anterior del art. 6 del Reg. (CE) 2004/460, el Consejo de Administración de ENISA estaba compuesto por "un representante de cada Estado miembro, tres representantes nombrados por la Comisión, así como por tres representantes propuestos por la Comisión y nombrados por el Consejo sin derecho a voto, cada uno de los cuales representará a uno de los siguientes grupos: a) sector de las tecnologías de la información y de la comunicación; b) grupos de consumidores; c) expertos académicos en seguridad de las redes y de la información".
61. Art. 15, apdo. 1, Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de la programación de ENISA[62], así como con aquellas de nombramiento, prórroga o eventual cese del director ejecutivo de la Agencia[63].

El Consejo de Administración está asistido por un comité ejecutivo[64]. Este órgano, compuesto por cinco miembros nombrados entre los miembros del Consejo, está llamado a desempeñar tres funciones básicas: (*i*) preparar las decisiones que deba tomar el Consejo; (*ii*) garantizar, junto con el Consejo, un seguimiento adecuado de las conclusiones y recomendaciones resultantes de las investigaciones realizadas por la Oficina Europea de Lucha contra el Fraude (OLAF); y (*iii*) asistir y asesorar al director ejecutivo en la aplicación de las decisiones del Consejo en materia administrativa y presupuestaria[65]. El legislador europeo no se limita a atribuir al Comité una función de asistencia frente a otros órganos, ya que —si es necesario por razones de urgencia— el Comité puede adoptar determinadas decisiones provisionales en nombre del Consejo de Administración (incluida la suspensión de la delegación de poderes de nombramiento)[66]. No obstante, esta capacidad de intervenir en situaciones urgentes se equilibra con la necesidad de someter todas las decisiones provisionales al Consejo para su aprobación o revisión en los tres meses siguientes a su adopción.

ENISA está dirigida por su director ejecutivo, que es independiente en el ejercicio de sus funciones[67]. Entre sus responsabilidades, el director de la Agencia tiene que (*i*) llevar a cabo la administración cotidiana de esta; (*ii*) aplicar las decisiones adoptadas por el Consejo de Administración; (*iii*) desarrollar y mantener contactos con las organizaciones empresariales y de consumidores activas en este ámbito; y (*iv*) intercambiar periódicamente puntos de vista e información con las instituciones, los órganos y organismos de la Unión sobre sus actividades en el ámbito de la ciberseguridad[68]. De hecho, el Reglamento (UE) 2019/881 permite al organismo crear grupos de trabajo ad hoc en apoyo de la labor de ENISA, compuestos por ex-

62. Funciones indicadas respectivamente en el art. 15, apdo. 1, letras c) y d), Reg. (UE) 2019/881.

63. Art. 15, apdo. 3, Reg. (UE) 2019/881. Además, en presencia de circunstancias excepcionales, el apdo. 3 permite al Consejo de Administración suspender temporalmente la delegación de poderes de nombramiento al director ejecutivo (así como a cualquier persona subdelegada).

64. Art. 19, apdo. 1, Reg. (UE) 2019/881.

65. Art. 19, apdo. 3, Reg. (UE) 2019/881.

66. Sin embargo, el art. 19, apdo. 7, Reg. (UE) 2019/881, especifica: "El Comité Ejecutivo no tomará una decisión en nombre del Consejo de Administración que deba ser aprobada por una mayoría de dos tercios del Consejo de Administración".

67. Art. 20, apdo. 1, Reg. (UE) 2019/881.

68. Art. 20, apdo. 2, Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

pertos (enviados también por las autoridades competentes de los Estados miembros)[69], o bien —previo consentimiento de la Comisión, el Consejo y los Estados miembros interesados[70]— una o varias oficinas locales, en la medida en que sean necesarias para llevar a cabo las tareas de ENISA de manera eficiente y eficaz (sobre la base de un análisis coste-beneficio adecuado).

Por último, para completar el análisis del marco organizativo de la Agencia, es necesario abordar ahora otros dos componentes innovadores introducidos por la Ley de Ciberseguridad, a saber: el Grupo Consultivo de ENISA y la red de funcionarios de enlace nacionales. El primero es un órgano compuesto por expertos que representan determinadas categorías de intereses que el Reglamento (UE) 2019/881 identifica sin pretender ser exhaustivo, esto es, expertos que trabajan en el sector de las TIC, proveedores de redes o servicios de comunicaciones electrónicas disponibles al público, pymes, operadores de servicios esenciales, organizaciones de consumidores y expertos académicos en ciberseguridad[71]. El Grupo Consultivo de ENISA está flanqueado por el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad, compuesto por un grupo de personas seleccionadas por la Comisión —y no por el Consejo de Administración de la Agencia, como el anterior— entre expertos reconocidos tras una convocatoria abierta y transparente[72].

El último elemento estratégico dentro de la Agencia es la red de funcionarios de enlace nacionales, un organismo creado para superar las barreras informativas y geográficas dentro de la Unión[73]. Esta red actúa para crear un flujo bidireccional de información entre los Estados miembros y ENISA, de modo que las mejores prácticas, las actualizaciones normativas, las amenazas y las estrategias de mitigación se compartan oportunamente, garantizando así que todos los Estados miembros estén equipados para hacer frente a los retos de seguridad de manera coordinada y coherente.

3.2. Los centros europeos de seguimiento y gestión de crisis cibernéticas

La gestión de crisis cibernéticas en la Unión Europea es un reto complejo y polifacético que implica a una amplia gama de actores a nivel nacio-

69. Art. 20, apdo. 4, Reg. (UE) 2019/881.
70. Art. 20, apdo. 5, Reg. (UE) 2019/881.
71. Art. 21, apdo. 1, Reg. (UE) 2019/881.
72. Art. 22 Reg. (UE) 2019/881.
73. Art. 23 Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

nal, europeo e internacional. En este contexto, la red de equipos de respuesta a incidentes de seguridad informática (red CSIRT) y la red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad (EU-CyCLONe) surgen como pilares clave de la respuesta europea a las ciberamenazas.

Por lo que respecta a los equipos de respuesta a incidentes de seguridad informática, la Directiva NIS2 pretende establecer un marco sólido para garantizar que cada Estado miembro cuente con uno o varios CSIRT adecuadamente equipados en términos de recursos humanos, técnicos y financieros para hacer frente a las amenazas de ciberseguridad de manera eficaz a través de una infraestructura de comunicación e información resistente[74]. Entre las tareas asignadas por la Directiva 2022/2555 a los CSIRT individuales se incluyen las de (*i*) supervisar y analizar las amenazas, vulnerabilidades e incidentes cibernéticos a nivel nacional y, previa solicitud, asistir a las partes interesadas esenciales e importantes en la supervisión en tiempo real de sus sistemas informáticos o de red; (*ii*) emitir alertas tempranas, alertas y avisos para difundir información sobre ciberamenazas, vulnerabilidades e incidentes entre las partes interesadas esenciales e importantes; (*iii*) asistir y responder a las partes interesadas esenciales e importantes; y (*iv*) participar en la red CSIRT y prestar asistencia mutua a otros miembros de la misma cuando la soliciten[75]. Esta última, que debe ser reconocida como un elemento central indiscutible en la infraestructura europea de ciberseguridad, no solo es el lugar natural para el intercambio de información pertinente sobre incidentes, cuasiincidentes, ciberamenazas, riesgos y vulnerabilidades, sino que también puede asumir la tarea de prestar asistencia operativa a los Estados miembros para hacer frente a un incidente con efectos potencialmente transfronterizos[76].

Por otra parte, el establecimiento de la red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad (EU-CyCLONe) fue dispuesto por la Directiva NIS2 con el fin de apoyar la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo, y cons-

74. Art. 10, apdo. 1, Dir. (UE) 2022/2555. Cabe destacar que, hasta la fecha, nada menos que 580 CSIRT están operativos a escala europea (89 de ellos solo en España). Un mapa interactivo de la actividad de los CSIRT es ofrecido por https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map.

75. Art. 10, apdo. 3, Dir. (UE) 2022/2555. Además de las que nos ocupan, la misma disposición obliga a los CSIRT a realizar determinadas tareas a petición de las partes interesadas esenciales e importantes. Entre ellas, cabe destacar las siguientes: (i) asistir a las entidades NIS2 en la supervisión en tiempo real o cuasireal de su red y sistemas de información, y (ii) proporcionar una exploración proactiva de los sistemas de redes y de información de la entidad afectada para detectar vulnerabilidad que puede tener una repercusión significativa.

76. Art. 3, letras f)-h), Dir. (UE) 2022/255.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

tituye hoy uno de los pilares clave incluidos en la más reciente estrategia de gestión de crisis cibernéticas de la Unión[77]. La red EU-CyCLONe está formada por representantes de las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y, en casos de especial relevancia, también de la Comisión (que siempre participa en las actividades de EU-CyCLONe en calidad de observador)[78]. Se trata de una red de coordinación diseñada para garantizar la participación de las principales autoridades nacionales de gestión de crisis de ciberseguridad, con una plataforma para la cooperación operativa y la coordinación entre los Estados miembros, la Comisión y ENISA.

Las competencias de la red NIS2 son similares a las ya destacadas en relación con los CSIRT, con la diferencia de que la presencia de un ciberataque a gran escala exige inevitablemente una mayor coordinación entre los Estados miembros, lo que a menudo requiere una coordinación a nivel político entre los dirigentes institucionales de los Estados miembros y de la Unión. En tal escenario, las capacidades de la infraestructura CyCLONe se ponen a prueba anualmente mediante ejercicios periódicos, como el *Blueprint Operational Level Exercise* (*Blue OLEx*), que reúne a los altos directivos de las autoridades competentes de los veintisiete Estados miembros para probar la eficacia de los procedimientos de respuesta a las cibercrisis[79].

Junto a las dos primeras infraestructuras, pronto se añadirá una tercera, la red de centros de operaciones de ciberseguridad (SOC, por sus siglas en inglés)[80]. Se trata de una red compuesta por centros dotados de profesionales de la seguridad de las TIC capaces de vigilar 24 horas al día, 7 días a la semana, toda la infraestructura informática de una organización, con el fin de hacer frente de la manera más rápida y eficaz posible a cualquier incidente o amenaza en tiempo real. Así pues, a diferencia de las estructuras abordadas anteriormente, que, como hemos visto, tienden a activarse en caso de crisis, los SOC están siempre activos y garantizan —en una lógica de colaboración— la mayor e indispensable eficacia de la red CSIRT y CyCLONe.

77. Art. 16, apdo. 1, Dir. (UE) 2022/2555.

78. Art. 16, apdo. 2, Dir. (UE) 2022/2555.

79. Entre los ejercicios *Blue OLEx* más recientes figuran los que tuvieron lugar en Lituania en 2022 (https://www.enisa.europa.eu/news/blue-olex-2022-tests-the-standard-operating-procedures-of-the-eu-cyclone) y en los Países Bajos en 2023 (https://www.enisa.europa.eu/news/blue-olex-2023-getting-ready-for-the-next-cybersecurity-crisis-in-the-eu).

80. Se hace referencia a un nuevo paquete normativo europeo que se está aprobando, conocido como *Cyber Solidarity Act* (CSA), que —entre otras cosas— ha previsto una financiación sustancial para la creación de SOC nacionales subordinados a la futura formación de SOC transfronterizos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

4. El marco europeo de certificación de la ciberseguridad

El Reglamento (UE) 2019/881 dedica todo el Título III (arts. 46-65) al marco europeo de certificación de la ciberseguridad, demostrando así la voluntad de la UE de consolidar su posición de "superpotencia regulatoria global" (Bradford, 2015: 178; Cantero Gamito, 2018: 396; Munkøe y Mölder, 2022: 73). Antes de la adopción de este reglamento, la Unión no contaba con un sistema de certificación unificado para la seguridad de los productos y sistemas TIC, sino que se basaba principalmente en las normas internacionales y de certificación establecidas por la Organización Internacional de Normalización (ISO)[81] y la Comisión Electrotécnica Internacional (CEI)[82]. En concreto, la seguridad de este tipo de productos y sistemas estaba garantizada tanto por el cumplimiento del "Criterio Común" (la ISO/IEC 15408), una norma internacional ampliamente reconocida para la evaluación de productos de TIC de uso generalizado en todos los Estados miembros[83], como por el cumplimiento de normas de certificación diseñadas para satisfacer necesidades específicas y propias de cada sector (como, por ejemplo, el estándar IEC 62443 sobre sistemas de control industrial). Dado que la presencia de estos espacios ha permitido fijar un nivel europeo de seguridad para los productos, sistemas y procesos TIC de media elevado, pero no uno capaz de salvar eficazmente las diferencias entre los distintos países miembros, el *Cybersecurity Act* pretendía armonizar las prácticas de certificación en materia de ciberseguridad mediante el desarrollo de una disciplina ambiciosa e innovadora.

En general, el marco europeo de certificación de la ciberseguridad tiene un doble objetivo: (*i*) aumentar la confianza en los productos, servicios y procesos de las TIC que han sido certificados a través de los sistemas

81. La Organización Internacional de Normalización (ISO) es una entidad independiente, no gubernamental, con sede en Ginebra y compuesta por organismos nacionales de normalización de 164 países, fundada en 1947 con el objetivo de elaborar y publicar normas internacionales que abarquen casi todos los aspectos de la tecnología y la fabricación.

82. La Comisión Electrotécnica Internacional (CEI) es una organización mundial fundada en Londres en 1906 (más tarde se trasladó también a Ginebra, en 1948) con el objetivo de elaborar normas internacionales para fomentar la interoperabilidad, seguridad y eficiencia energética de los productos eléctricos y electrónicos. En la actualidad, en colaboración con otras organizaciones como ISO e ITU, la CEI apoya la innovación tecnológica y el comercio nacional, al tiempo que garantiza la seguridad de los consumidores y la sostenibilidad medioambiental.

83. Se trata de una norma de seguridad genérica que contiene un conjunto común de requisitos para las funciones de seguridad de los productos y sistemas TIC y para las medidas de garantía que se les aplican, y que puede aplicarse en cualquier ámbito relacionado con la seguridad de los productos o servicios TIC.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

europeos de certificación de la ciberseguridad, y, al mismo tiempo[84], (*ii*) evitar la multiplicación o el solapamiento de regímenes nacionales de certificación de la ciberseguridad y reducir así los costes para las empresas que operan en el mercado único digital (Chiara, 2022: 120). Para lograrlo, el legislador europeo estableció el marco de certificación de la ciberseguridad, confiando a la Comisión la tarea de preparar un programa de trabajo evolutivo de la Unión destinado a determinar las prioridades estratégicas de los futuros sistemas europeos de certificación de la ciberseguridad[85]. En concreto, el Reglamento (UE) 2019/881 fijó como objetivo de este programa la identificación de una lista de productos, servicios y procesos de TIC que pudieran beneficiarse de su inclusión en un sistema de certificación[86], al tiempo que estableció de forma analítica los criterios que debían utilizarse para identificarlos[87].

Más relevante para el presente estudio, vale la pena examinar de cerca el marco proporcionado por el Reglamento (UE) 2019/881 en relación con la preparación, adopción y revisión de un sistema europeo de certificación de la ciberseguridad. En particular, el artículo 49 del *Cybersecurity Act* encomienda a ENISA, a petición de la Comisión, la tarea de preparar —tras debatirlo con todas las partes interesadas[88]— una propuesta de sistema capaz de cumplir los objetivos, niveles de fiabilidad y elementos del sistema identificados por el propio reglamento[89]. Sobre esta base, la Comisión podrá finalmente adoptar los actos de ejecución necesarios para la utilización del sistema europeo de certificación[90].

Llegados a este punto, antes de introducir el contenido del primer sistema de certificación de la ciberseguridad de ámbito europeo aproba-

84. El art. 46, apdo. 1, Reg. (UE) 2019/881 establece, de hecho, lo siguiente: "Se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC".

85. Art. 47, apdo. 1, Reg. (UE) 2019/881.

86. Art. 47, apdo. 2, Reg. (UE) 2019/881.

87. Art. 47, apdo. 3, Reg. (UE) 2019/881.

88. El art. 49, apdo. 3, Reg. (UE) 2019/881, prevé en particular: "A la hora de preparar las propuestas de esquema ENISA consultará a todas las partes interesadas mediante un proceso de consulta oficial transparente e inclusivo".

89. Art. 49, apdo. 1, Reg. (UE) 2019/881. Para ello, ENISA se sirve del Grupo Europeo de Certificación de la Ciberseguridad (GECC), que proporciona a la Agencia asistencia y asesoramiento experto en relación con la propuesta de sistema mediante la elaboración de dictámenes no obligatorios ni vinculantes (art. 49, apdo. 6).

90. Art. 49, apdo. 7, Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

do el pasado mes de febrero de 2024[91], se considera necesario centrarse en dos componentes esenciales del Reglamento (UE) 2019/881, referidos tanto a los niveles de fiabilidad de los sistemas de certificación europeos como a la delicada cuestión de su obligatoriedad.

Con relación al primer perfil, el *Cybersecurity Act* prevé que el esquema europeo de certificación podrá especificar niveles de garantía "básico", "sustancial" o "elevado", según el nivel correspondiente de riesgo asociado al uso previsto de un producto, servicio o proceso de TIC en términos de probabilidad y repercusiones de un incidente[92]. En particular, yendo por orden: (*i*) el nivel de garantía básico asegura que los productos, servicios o procesos de TIC cumplen con los requisitos de seguridad y se evalúan a un nivel destinado a minimizar "los riesgos básicos conocidos de ciberincidentes y ciberataques"[93]; (*ii*) el nivel de garantía "sustancial" comparte los mismos supuestos que el anterior, pero certifica que los productos, servicios o procesos son capaces de minimizar "los riesgos de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados"[94]; (*iii*) por último, el nivel de fiabilidad "elevado" garantiza que dichos productos, servicios o procesos son capaces de "minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables"[95]. El esquema descrito ha sido adoptado por el reciente esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) aprobado por el Reglamento de Ejecución (UE) 2024/482. En síntesis, siguiendo la disciplina del *Cybersecurity Act*, este esquema ha ideado cinco

91. Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC).

92. Art. 52, apdo. 1, Reg. (UE) 2019/881.

93. Art. 52, apdo. 5, Reg. (UE) 2019/881. En lo que respecta a este nivel de garantía, la disposición objeto de examen prevé al menos una revisión de la documentación técnica como actividad de evaluación. Por otra parte, conviene precisar que el posterior art. 53, apdo. 1, permite realizar una autoevaluación de la conformidad bajo la responsabilidad exclusiva del fabricante o proveedor en relación con productos, servicios y procesos de TIC que presenten un bajo riesgo correspondientes al nivel de garantía "básico".

94. Art. 52, apdo. 6, Reg. (UE) 2019/881. En este caso, las actividades de evaluación son distintas, puesto que "incluirán al menos: la revisión para demostrar la ausencia de las vulnerabilidades conocidas públicamente y la comprobación de que los productos, servicios o procesos de TIC aplican correctamente las funcionalidades de seguridad necesarias".

95. Art. 52, apdo 7, Reg. (UE) 2019/881. Las actividades de evaluación vinculadas al nivel de fiabilidad "elevado" son evidentemente más profundas, ya que, a diferencia de las previsibles, exigen por lo menos "la revisión de la improcedencia de las vulnerabilidades conocidas públicamente, la comprobación de que los productos, procesos o servicios de TIC aplican correctamente la necesaria funcionalidad de seguridad, con las tecnologías más avanzadas, y la evaluación de su resistencia a atacantes expertos mediante pruebas de penetración".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

perfiles de confianza (AVA_VAN)[96] flanqueados por los siete niveles de los "criterios comunes" (EAL), tal y como se muestra en la siguiente tabla:

ISO/IEC 15408 (criterios comunes)	**EUCC 2024**
EAL 1 (funcionalidad probada)	**AVA_VAN.1,AVA_VAN.2** Nivel de garantía "sustancial"
EAL 2 (estructuralmente probado)	
EAL 3 (probado y verificado metódicamente)	
EAL 4 (diseñado, probado y revisado metódicamente)	**AVA_VAN.3, AVA_VAN.4, AVA_VAN.5** Nivel de garantía "elevado"
EAL 5 (diseñado y probado semiformalmente)	
EAL 6 (diseño verificado y probado semiformalmente)	
EAL 7 (diseño verificado y probado formalmente)	

Fuente: elaboración propia.

Como se puede observar, en relación con el sistema inicialmente previsto en el Reglamento (UE) 2019/881, el EUCC no prevé la posibilidad de emitir certificaciones de nivel "básico". Como consecuencia inmediata, el esquema de certificación introducido en 2024 excluye la posibilidad de cualquier tipo de autoevaluación de la conformidad bajo la responsabilidad exclusiva del fabricante o proveedor en relación con productos, servicios y procesos de TIC[97]. Esta elección de las instituciones europeas es de agradecer ante el incremento exponencial de los ciberriesgos en los últimos cinco años, en los que, además de un aumento significativo de las capacidades ofensivas de los atacantes, ha cambiado visiblemente

96. Art. 2, apdo. 8), Reg. (UE) 2024/482: "'nivel AVA_VAN': nivel de garantía de análisis de vulnerabilidades que indica el grado de actividades de evaluación de la ciberseguridad llevadas a cabo para determinar el nivel de resistencia ante el posible aprovechamiento de defectos o debilidades del objeto de evaluación en su entorno operativo, tal como se establece en los criterios comunes".

97. Véase *supra* nota 93 (art. 52, apdo. 5, Reg. [UE] 2019/881).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

el escenario político internacional en el que nació el Reglamento (UE) 2019/881.

Como ya se ha mencionado, otro elemento esencial del Reglamento se encuentra en la elección del legislador europeo de especificar lo siguiente: "La certificación de la ciberseguridad será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros"[98]. En esta fase inicial, el carácter voluntario de las certificaciones de ciberseguridad debe interpretarse desde la perspectiva de un equilibrio preciso entre las necesidades de seguridad de la Unión y las elevadas cargas que supone para los particulares la obtención de tales certificados. Sin embargo, puesto que el Reglamento (UE) 2019/881 encarga a la Comisión evaluar periódicamente la eficacia y el uso de los regímenes europeos de certificación de la ciberseguridad, así como la posible necesidad de hacer uno obligatorio mediante las disposiciones pertinentes de la Unión[99], cabe recordar que, "incluso permaneciendo voluntarios, los esquemas pueden utilizarse para cumplir con los requisitos obligatorios de otros actos jurídicos" (Chiara, 2022: 122).

5. Conclusiones

El análisis realizado en las páginas precedentes demuestra que el marco jurídico europeo pretende desarrollar algo mucho más ambicioso que una mera disciplina destinada a reforzar la capacidad individual de cada Estado miembro para resistir a los ciberataques. Por el contrario, partiendo de la base de que "el todo no siempre es igual a la suma de las partes", el renovado marco jurídico europeo de la ciberseguridad entiende esta como una fuerza colectiva resultante de la interacción y cooperación —tanto horizontal como vertical— entre todas las entidades públicas y privadas implicadas. Desde la publicación de la primera estrategia de ciberseguridad en 2013, la Unión Europea ha logrado en poco tiempo establecer una infraestructura de defensa capaz de hacer frente a los retos de este nuevo siglo de una manera, sin duda, ambiciosa. Sin embargo, a pesar de ello, en la actualidad resulta extremadamente difícil imaginar cuál será el futuro próximo de la ciberseguridad europea. Esto no solo tiene que ver con la naturaleza variable de la materia, sino también (y quizá sobre todo) con cuestiones que pueden considerarse meta- o extralegales.

98. Art. 56, apdo. 2, Reg. (UE) 2019/881.
99. Art. 53, apdo. 3, Reg. (UE) 2019/881.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

En un contexto en el que la tendencia del escenario político internacional parece deteriorarse cada vez más, para poder realizar siquiera parte de sus objetivos, la Unión Europea está llamada a replantearse algunas de las cuestiones que hasta ahora han demostrado ser claros obstáculos en el camino de la integración. Partiendo de la base de que la Unión, para superar estos retos, está llamada a replantearse sus fundamentos políticos más que jurídicos, es inevitable cuestionarse la conveniencia de relajar la rigidez de la actual prerrogativa estatal en materia de seguridad nacional. En este contexto, la consecución de los objetivos de cooperación y solidez de lo nuevo que persigue la actual infraestructura europea de ciberseguridad exige un replanteamiento radical del concepto de seguridad europea, capaz de responder a las diferentes necesidades de todos los Estados miembros. Por ello, la mayor atención prestada por el legislador europeo en los últimos años a esta cuestión debe considerarse como el punto de partida (y no de llegada) de una revolución que es política y cultural antes que jurídica.

6. Bibliografía

Ballestero, F. (2022). Cómo mejorar la ciberseguridad en España. Pasos ante una gran oportunidad. *Boletín económico de ICE*, 3148, 35-49. Disponible en https://doi.org/10.32796/bice.2022.3148.7457.

Bradford, A. (2015). Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, 42, 158-173. Disponible en https://doi.org/10.1016/j.irle.2014.09.004.

Cantero Gamito, M. (2018). Europeanization through Standardization: ICT and Telecommunications. *Yearbook of European Law*, 37, 395-423. Disponible en https://doi.org/10.1093/yel/yey018.

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, 36 (2), 118-137. Disponible en https://doi.org/10.1080/13600869.2022.2060468.

Comisión de las Comunidades Europeas. (2000). *Comunicación de la Comisión al Consejo y al Parlamento Europeo - Puesta al día sobre eEurope2002* (29-11-2000). Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0783.

Comisión de las Comunidades Europeas. (2001). *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones -Seguridad de las redes y de la información: Propuesta para un enfoque político europeo* (6-6-2001). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52001DC0298.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Comisión de las Comunidades Europeas. (2006). *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones - Una estrategia para una sociedad de la información segura* - "Diálogo, asociación y potenciación" (31-5-2006). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52006DC0251.

Comisión de las Comunidades Europeas. (2009). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información. "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia"* (30-3-2009). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52009DC0149.

Comisión Europea. (2013). *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro* (7-2-2013). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001.

Comisión Europea. (2017). *Comunicación conjunta al Parlamento Europeo y al Consejo - Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE* (13-9-2017). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450.

Comisión Europea. (2020). *Comunicación conjunta al Parlamento Europeo y al Consejo - La Estrategia de Ciberseguridad de la UE para la Década Digital* (16-12-2020). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020JC0018.

Denardis, N. (2020). *The Internet in Everything. Freedom and security in a world with no off switch*. Yale: University Press.

Fernández García, E. (2022). Desafíos jurídicos interdisciplinares de la ciberseguridad nacional: Apuntes *de lege ferenda. Anuario de la Facultad de Derecho. Universidad de Extremadura*, 37, 75-118. Disponible en https://doi.org/10.17398/2695-7728.37.75.

Floridi, L. (2015). The Onlife Manifesto. *Being Human in a Hyperconnected Era*. Disponible en https://link.springer.com/book/10.1007/978-3-319-04093-6.

Fuertes, M. (2022). *Metamorfosis del Estado. Maremoto digital y ciberseguridad*. Madrid: Marcial Pons.

International Telecomunication Union. (2020). *Global Cybersecurity Index (GCI)*. Disponible en https://www.itu.int.

Juncker, J.-C. (2017). State of the Union address. *European Commission*, 6-9-2017. Disponible en https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_17_3165.

Kaiser, E. (2023). The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations. *MediaLaws*, 1, 343-357. Disponible en 1-23-RDM.pdf.

Munkøe, M. y Mölder, H. (2022). La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar los nuevos retos? *Revista CIDOB d'Afers Internacionals*, 131, 69-94. Disponible en https://doi.org/10.24241/rcai.2022.131.2.69.

Perrow, C. (1984). Normal accidents. *Living with high-risk technologies*. Princeton: University Press.

Wessel, R.A. (2015). Towards EU Cybersecurity Law: Regulating a New Policy Field. En N. Tragourias y R. Buchan (dirs.). *Research Handbook on International Law and Cyber Space* (pp. 403-425). Cheltenham: Edward.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6