# CAPÍTULO III

# La normativa y organización española sobre ciberseguridad: su incidencia en la Administración local

**Anxo Varela Hernández**
*Profesor del Departamento de Derecho Público y Teoría del Estado.*
*Universidad de Santiago de Compostela*

**SUMARIO. 1. Introducción: la ciberseguridad como elemento estratégico para el Estado de derecho. 2. La transposición en el ordenamiento jurídico español de la Directiva NIS.** 2.1. Marco normativo español: el Real Decreto-ley 12/2018, su desarrollo reglamentario y el papel de los centros de respuesta ante incidentes (CSIRT). 2.2. La evolución hacia la Directiva NIS 2 y su implementación en España. **3. La relevancia de la ciberseguridad en el ámbito de la seguridad nacional y de las Administraciones públicas.** 3.1. La Ley de Seguridad Nacional y la Estrategia de Seguridad Nacional. 3.2. El Esquema Nacional de Seguridad. Su posible incidencia en la Administración local. 3.3. El Plan Nacional de Ciberseguridad y otros documentos de interés. 3.4. La Administración pública y las infraestructuras críticas: especial atención a la Ley 8/2011 y a su reglamento de desarrollo. **4. Entidades clave en materia de ciberseguridad en España.** 4.1. El Centro Criptológico Nacional (CCN) y su apoyo a las corporaciones locales. 4.2. El Instituto Nacional de Ciberseguridad (INCIBE) y la ciberseguridad operativa. 4.3. Otros órganos de relevancia: del Centro Nacional de Protección de Infraestructuras Críticas al Consejo Nacional de Ciberseguridad. **5. Conclusiones. 6. Bibliografía.**


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

## 1. Introducción: la ciberseguridad como elemento estratégico para el Estado de derecho

La ciberseguridad se ha convertido en un elemento estratégico para el funcionamiento del Estado en todos sus niveles, incluido aquel más próximo al ciudadano: las Administraciones locales. Aunque la digitalización ha permitido a los entes locales mejorar sus servicios, optimizar sus recursos y acercarse más a la ciudadanía, también ha multiplicado su exposición a los riesgos en el ciberespacio[1], y ha hecho crecer la dependencia de la tecnología y de otros elementos como la red eléctrica —tal y como se pudo comprobar con el apagón sufrido en España a finales de abril del año 2025—, elementos estos que hacen necesario examinar la cuestión con cierto grado de detenimiento.

Sin ir más lejos, el 14 de abril de 2025 el Ayuntamiento de Boqueixón, en Galicia, sufrió un ataque que logró duplicar dos de las líneas telefónicas municipales, entre ellas la del propio alcalde. Una semana antes, era el Ayuntamiento de Teo —próximo a la capital gallega— el que alertaba de un intento de *phishing*, pues a través de la suplantación de la identidad del personal municipal se solicitó a uno de los contratistas habituales de la corporación municipal el envío de documentación. No se trata de dos sucesos excepcionales o eventuales, sino que las Administraciones locales, y particularmente los pequeños ayuntamientos, se han convertido en un blanco fácil por sus menores capacidades económicas y humanas y, por tanto, por su resistencia mínima. De hecho, según la Agencia para la Modernización Tecnológica de Galicia (AMTEGA), el correo electrónico sigue siendo la principal vía de entrada de los ciberdelincuentes en las Administraciones públicas, y, según el Centro Criptológico Nacional, este recibió información de más de 1400 incidentes de ciberseguridad en las Administraciones autonómica y locales de Galicia en el año 2023[2]. A estos efectos, por cierto, puede resultar interesante la consulta del Informe sobre la Cibercriminalidad en España del año 2023 —que es el último año publicado—[3].

1. En el año 2023, según datos del Centro Criptológico Nacional, hubo más de 1400 incidentes en las Administraciones locales gallegas, tal y como se puede comprobar en el siguiente enlace: https://amtega.xunta.gal/es/noticia/el-centro-criptoloxico-nacional-recibio-informacion-de-mas-de-1400-incidentes-de (fecha de última consulta: 15/04/2025).

2. Como destaca la siguiente nota de prensa de la propia AMTEGA: https://amtega.xunta.gal/es/noticia/el-centro-criptoloxico-nacional-recibio-informacion-de-mas-de-1400-incidentes-de.

3. Se puede consultar en el siguiente enlace: https://www.interior.gob.es/opencms/es/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas/informe-sobre-la-cibercriminalidad-en-espana/.


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

También otras Administraciones han sido objeto de ciberataques[4]. En el caso de la Xunta de Galicia, en el pasado año 2024 sus plataformas de seguridad perimetral neutralizaron cerca de 237 millones de intentos de ataque, un 42 % más que los 166 millones registrados en 2023, y el 9 de julio de 2024 los datos de más de 5 mil profesionales de la sanidad pública andaluza quedaron al descubierto por un ciberataque que culminó con la solicitud de un rescate[5].

No se trata, como sabemos, de una cuestión con incidencia nacional. Como ejemplo, el ciberataque a diferentes aeropuertos europeos, entre los que destacan los de las ciudades de Londres, Berlín y Bruselas, en septiembre de 2025. El análisis de la cuestión desde la perspectiva europea se encuentra en el "Informe de 2024 sobre el estado de la ciberseguridad en la Unión"[6], que se constituye como el primer informe sobre el estado de la ciberseguridad en la Unión Europea, elaborado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y que, por cierto, ha ido incrementando su protagonismo de forma progresiva (Fuertes López, 2022: 111).

En este contexto, es imprescindible comprender la arquitectura normativa y organizativa que estructura la protección frente a las ciberamenazas en España, y su incidencia en las propias Administraciones locales, destacando la necesidad de adoptar medidas coordinadas para su protección[7].

Así pues, este capítulo ofrece un recorrido sistemático por los principales elementos normativos y organizativos que conforman el modelo español de ciberseguridad, con especial atención a su aplicación en el ámbito local, y aunque se hará referencia a instrumentos supranacionales, como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, no se profundizará en ellos con sumo detalle, ya que serán analizados en otros capítulos de este libro colectivo.

4. Misma suerte que corren las empresas privadas: según un estudio elaborado por la empresa Zerod, un *marketplace* de *ethical hackers* español, un 68 % de las empresas españolas sufrió al menos un intento de ciberataque en 2024.

5. Todo ello se puede consultar en la siguiente web: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-contra-el-servicio-andaluz-de-salud (fecha de última consulta: 15/04/2025).

6. Disponible en el siguiente enlace: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union (fecha de última consulta: 17/04/2025).

7. Sobre los conceptos de coordinación y cooperación, *vid*. Almeida Cerreda (2024).


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

La finalidad de este capítulo no es, por tanto, describir únicamente normas y organismos, sino también evidenciar la necesidad de una visión integral y descentralizada de la ciberseguridad, que permita a los Gobiernos locales ejercer sus competencias con seguridad, autonomía y confianza digital. En un entorno cada vez más interconectado y vulnerable, solo desde una gobernanza coordinada y una estrategia normativa coherente podrá garantizarse una Administración pública verdaderamente segura, resiliente y al servicio de la sociedad.

Para ello, es fundamental comprender el amplio concepto de la "ciberseguridad", ya que en el contexto actual, donde proliferan fenómenos como la desinformación, la manipulación algorítmica o el espionaje digital, la ciberseguridad adquiere una dimensión también política y social, en tanto en cuanto su finalidad última no debe ser, exclusivamente, evitar daños técnicos, sino también garantizar la confianza de la ciudadanía en las instituciones públicas, proteger derechos fundamentales (como la privacidad) y salvaguardar el buen funcionamiento y la protección de las bases sobre las que se sienta el propio Estado de derecho. O lo que es lo mismo, en este concepto amplio de ciberseguridad podemos encuadrar las acciones, métodos e instrumentos para garantizar en soportes tecnológicos la confidencialidad, integridad, disponibilidad y autenticación de la información y de los servicios, pero no únicamente (Fernández Rodríguez, 2018: 53).

Esta visión amplia es indispensable para que la Administración pública local, en particular los ayuntamientos, puedan responder a los retos actuales de forma eficaz y coherente. Con todo, no debe pensarse que las cuestiones de ciberseguridad son sectoriales y no interfieren en la normativa administrativista. De hecho, son un componente interdisciplinar presente en todo el ordenamiento jurídico. Muestra de ello es la preocupación que, entre otras, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, presta a las ciberamenazas, permitiendo la ampliación general de los plazos de los procedimientos administrativos cuando por la acción de un ciberincidente se hayan visto gravemente afectados los servicios y sistemas utilizados para la tramitación de los procedimientos y el ejercicio de los derechos de los interesados, tal y como reza su artículo 32.5[8]. En el ámbito de la Unión,

8. Este párrafo fue añadido por el Real Decreto-ley 6/2022, de 29 de marzo, por el que se adoptan medidas urgentes en el marco del Plan Nacional de respuesta a las consecuencias económicas y sociales de la guerra en Ucrania, lo que corrobora que la ciberseguridad es un elemento protagonista en los conflictos bélicos del presente.


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

podemos destacar la reciente aprobación del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero, más conocido como Reglamento DORA.

## 2. La transposición en el ordenamiento jurídico español de la Directiva NIS

La irrupción del ciberespacio[9] como un ámbito estratégico para la economía, la seguridad y los derechos fundamentales, ha obligado a los Estados y organizaciones internacionales a adoptar normativas específicas para garantizar la integridad de las redes y sistemas de información.

En este contexto, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[10], más conocida como Directiva NIS (por su acrónimo en inglés *Network and Information Security*), fue la primera norma de la Unión Europea en abordar de forma integral el fenómeno de la ciberseguridad, estableciendo obligaciones comunes para todos los Estados miembros. Esta respondía a la creciente necesidad de proteger las redes y sistemas de información que sustentan los servicios esenciales en sectores críticos como la energía, el transporte o la infraestructura digital.

Su principal objetivo, como se desgrana en otro de los capítulos de este libro, era alcanzar un nivel común elevado de seguridad en las redes y en los sistemas de información en la Unión, como medio para garanti-

9. El informe "La Ciberseguridad Nacional, un compromiso de todos", elaborado por el INCIBE, define en su página 12 al ciberespacio como el "conjunto de medios y procedimientos basados en las Tecnologías de la Información y la Comunicación (TIC) configurados para la prestación de servicios", que se encuentra vertebrado sobre tres capas superpuestas: la capa física, la capa lógica y la capa social. Por todo ello, la perfección de los sistemas de control que lo componen es relevante a efectos de garantizar "la provisión de aquellos servicios esenciales para la actividad socioeconómica de cualquier nación, y en especial aquellos ligados a sus infraestructuras críticas", como, de nuevo, reconoce dicho informe, que está disponible en el siguiente enlace: https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf (fecha de última consulta: 15/04/2025). Dicho de otro modo, el ciberespacio es un lugar de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, con los riesgos que ello conlleva.

10. Y que, por cierto, ya no se encuentra en vigor, porque ha sido derogada por 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.


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

zar el funcionamiento del mercado interior. Para ello, se centraba especialmente en tres pilares: la mejora de las capacidades nacionales de ciberseguridad[11]; la creación de un marco de cooperación entre los Estados miembros; y la imposición de requisitos de seguridad y de notificación de incidentes a los operadores de servicios esenciales y a determinados proveedores de servicios digitales.

### 2.1. Marco normativo español: el Real Decreto-ley 12/2018, su desarrollo reglamentario y el papel de los centros de respuesta ante incidentes (CSIRT)

La Directiva ahora analizada reconocía la naturaleza transfronteriza de los riesgos cibernéticos y la interdependencia digital entre los Estados miembros, por lo que establecía un marco mínimo armonizado que debía ser completado por la legislación nacional de cada país. En España la Directiva fue transpuesta mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información[12]. Esta norma se convirtió en el instrumento jurídico clave para estructurar la respuesta nacional en materia de ciberseguridad, regulando no solo la seguridad de las infraestructuras digitales esenciales, sino también los mecanismos institucionales de prevención, supervisión y coordinación.

El decreto define, en primer lugar, el ámbito de aplicación de la norma, que incluye, en virtud de su artículo 2.2, tanto a los operadores de servicios esenciales[13], es decir, aquellos cuya actividad sea crítica para el mantenimiento de funciones sociales, sanitarias, económicas o de seguridad, como a los proveedores de servicios digitales[14], es decir, a los motores

11. Mediante el establecimiento, entre otros instrumentos, de los equipos de respuesta ante incidentes.

12. Aunque la fecha máxima de transposición era el 9 de mayo de 2018, España adaptó la directiva a su ordenamiento jurídico en el mes de septiembre de dicho año, y mediante la fórmula del real decreto-ley, un instrumento desde luego cuestionado por la previsión constitucional del artículo 86 de la Constitución Española, que reserva su utilización a los casos "de extraordinaria y urgente necesidad". Sobre la transposición de la directiva por otros Estados miembros, se debe consultar https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=CELEX:32016L1148&qid=1744745391231 (fecha de última consulta: 15/04/2025).

13. No debe olvidarse en este punto que, como afirma Fuertes López (2022: 30-31), pese a que el legislador ha ido precisando las naciones que conforman el término "esencial", estamos ante un concepto jurídico indeterminado cuya calificación dependerá del contexto existente, con sus correspondientes riesgos.

14. Conviene destacar en este punto que la norma remite a los órganos y procedimientos previstos en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, para la identificación de los servicios esenciales y de los operadores que los presten.


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

de búsqueda, servicios de computación en la nube y plataformas digitales, estableciendo obligaciones para todos estos sujetos.

Entre otras obligaciones, todas ellas previstas con carácter general en el artículo 16 del Real Decreto-ley analizado, podemos destacar la adopción de medidas técnicas y organizativas apropiadas y proporcionadas a los riesgos existentes; la notificación de incidentes con efectos significativos en la prestación de servicios (desarrollada de forma profusa en el título V); y la colaboración con las autoridades competentes y los equipos de respuesta a incidentes de seguridad (CSIRT), de los que hablaremos más adelante. Resulta interesante destacar en este punto la obligación destinada a que los operadores de servicios esenciales establezcan la persona, unidad u órgano colegiado responsable de la seguridad de la información, a efectos de que se mantenga una correcta colaboración e intercomunicación con la autoridad competente. Ello, sin duda, agiliza la respuesta e incluso la anticipación ante cualquier ciberamenaza.

Esta norma con rango de ley, aunque no es demasiado extensa, prevé también un sistema institucional complejo que articula distintos niveles de autoridad. En la cúspide se encuentra la autoridad competente (prevista en los artículos 9 y 10), que, dada la transversalidad de la ciberseguridad, será una u otra en función de si estamos ante un proveedor de servicios digitales (en donde será la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital), un operador de un servicio esencial que sea crítico (en donde ejercerá dicha labor la Secretaría de Estado de Seguridad, perteneciente al Ministerio del Interior), u operadores que, siendo esenciales, no sean críticos[15] (caso, este último, en donde se reconocen reglamentariamente autoridades sectoriales según el tipo de servicio esencial afectado).

Ese desarrollo del Real Decreto-ley ha venido dado por el Real Decreto 43/2021, de 26 de enero[16], que prevé en su artículo 3 aquellas autoridades competentes en función del ámbito sectorial. A modo de ejemplo, respecto al sector de la energía, ejercerá tales funciones el Ministerio para

15. Es decir, no han sido designados como tales según la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

16. El INCIBE se ha esforzado en desgranar los aspectos más relevantes del mismo en el siguiente enlace: https://www.incibe.es/incibe-cert/sobre-incibe-cert/FAQ-RD_43-2021#hay-un-regimen-sancionador (fecha de última consulta: 17/04/2025).

la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

En segundo término, destacan los CSIRT (por su nomenclatura en inglés *Computer Security Incident Response Team*)[17], o lo que es lo mismo, los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional[18]. El Real Decreto-ley 12/2018 otorga un papel central a los equipos de respuesta ante incidentes de seguridad informática, ya que, aunque el operador sigue siendo el responsable de resolver los incidentes y de actuar en la reposición de la normalidad de las redes y sistemas de información afectados, con su comunicación a los CSIRT se organiza de forma ágil la respuesta a dichos incidentes, pese a que el destinatario último de las notificaciones siempre será la autoridad competente respectiva. La normativa refuerza, entonces, su papel, otorgándoles funciones formales en el proceso de notificación de incidentes, y establece canales de cooperación obligatoria entre ellos, las autoridades competentes y los sujetos obligados. Además, el Real Decreto 43/2021 instrumenta esta coordinación a través de la Plataforma Nacional de Notificación y Seguimiento de Incidentes, de tal manera que los operadores no deben efectuar varias notificaciones en función de la autoridad a la que deban dirigirse, y establece el Esquema de Seguridad Nacional, sobre el que hablaremos más adelante, como punto de partida para cumplir la ley. Estamos, pues, frente a un claro ejemplo de la convergencia entre la regulación de datos y la de ciberseguridad.

Al igual que ocurre respecto de las autoridades competentes, los equipos de respuesta a incidentes varían en función de si estamos ante un operador de servicio esencial o no. En el ámbito español, destacan el CCN-CERT[19], dependiente del Centro Criptológico Nacional y especializado en la protección de organismos públicos y sectores estratégicos, y el INCIBE-CERT[20], dependiente del Instituto Nacional de Ciberseguridad, que actúa como equipo de respuesta de referencia para ciudadanos, empresas y operadores privados.

17. En Estados Unidos se los conoce como CERT (*Computer Emergency Response Team*).

18. Aunque la directiva los hace suyos, el concepto de "equipos de respuesta a incidentes de seguridad" ha evolucionado desde su nacimiento tras el considerado primer gran ciberataque mundial, provocado por el virus Morris, en 1988.

19. Como se ha dicho, el acrónimo CERT proviene de *Computer Emergency Response Team*.

20. Que durante el año 2024 gestionó un total de 97 348 incidentes de ciberseguridad, como se extrae de https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes (fecha de última consulta: 15/04/2025).


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

Uno de los elementos nucleares de la normativa en esta materia estriba en la coordinación y la cooperación exigidas, lo que demuestra que estos equipos no solo actúan como centros de respuesta ante incidentes, sino también como núcleos de conocimiento, detección temprana, prevención y asesoramiento técnico. De hecho, la propia norma configura un sistema nacional de ciberseguridad que se apoya, sobremanera, en los principios de colaboración público-privada, en la descentralización administrativa y en la responsabilidad compartida. Como muestra de ello, el artículo 14 conmina a la cooperación con otras autoridades con competencias en seguridad de la información, y con las autoridades sectoriales.

Huelga señalar que, en cumplimiento del artículo 21 de la Directiva 2016/1148, España ha establecido un régimen sancionador exhaustivo en el título VII del Real Decreto-ley 12/2018, previendo la responsabilidad directa de los operadores de servicios esenciales y de los proveedores de servicios digitales, con infracciones muy graves, graves y leves que oscilan entre el millón de euros o la amonestación[21], para lo que se tendrán en cuenta no solo el ámbito material que califica la gravedad de la propia sanción, sino también elementos tales como el grado de culpabilidad, la persistencia en la conducta infractora o el número de usuarios afectados, previstos todos ellos en el artículo 38.

### 2.2. La evolución hacia la Directiva NIS 2 y su implementación en España

A pesar del valor pionero de la Directiva NIS, con el paso de los años se identificaron diversas limitaciones en la normativa europea, como la cobertura insuficiente de sectores clave, las diferencias de aplicación entre Estados, la escasa cooperación práctica entre autoridades y la falta de obligaciones estrictas de supervisión. Como respuesta, la Comisión Europea propuso en 2020 una revisión completa del marco legal en esta materia, que dio lugar a la nueva 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, conocida como NIS 2[22].

Esta directiva, tal y como se desarrolla en otro de los capítulos de este libro, amplía de forma significativa el ámbito de aplicación de la norma

21. Aunque para las Administraciones públicas se prevé un régimen especial en el artículo 40.

22. El INCIBE, sobre el que hablaremos en otro de los epígrafes de este capítulo, ha dedicado un espacio web a resolver dudas acerca de la misma: https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2.


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

comunitaria anterior, incluyendo nuevos sectores como servicios postales, residuos, producción alimentaria o fabricación de productos críticos; y matizando elementos en relación con las propias Administraciones públicas, así como endureciendo las obligaciones de seguridad, reforzando los mecanismos de supervisión y sanción, y exigiendo a los Estados miembros mayor coherencia en la implementación. De hecho, en el ámbito sancionador, tal y como reza el considerando 131, la Unión Europea conmina a los Estados miembros a la imposición de sanciones penales, destacando, como resulta obvio, el necesario respeto por el principio *ne bis in idem*. Así pues, la Directiva NIS 2 representa un paso decisivo hacia una Unión Europea cibernéticamente más resiliente, con un modelo más homogéneo y efectivo, alineado con el nivel de amenaza actual, que pretende corregir las limitaciones reveladas con la transposición de la primaria Directiva NIS, analizada en el apartado anterior.

Pese a que en virtud del artículo 41 de la directiva en cuestión esta debía estar transpuesta a más tardar el 17 de octubre de 2024, en España la transposición de esta nueva directiva está en proceso. El Consejo de Ministros del martes 14 de enero de 2025 aprobó el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública, que, según reza la nota de prensa[23], será tramitado de urgencia para que pueda ser aprobado por el Gobierno, en segunda vuelta, cuanto antes, y dar de inmediato paso a su debate parlamentario.

La futura Ley de Coordinación y Gobernanza de la Seguridad prevé un ámbito de aplicación material amplio, pues en virtud de su artículo 3, que establece un criterio uniforme, resulta de aplicación a las entidades públicas o privadas que tengan su residencia fiscal en España, o que, teniendo su residencia en otro Estado de la Unión Europea, ofrezcan sus servicios o desarrollen su actividad en nuestro país. Diferencia, eso sí, entre entidades encuadradas en sectores considerados de alta criticidad para el normal funcionamiento de la vida social y económica del país, y entidades que pertenezcan a otros sectores de menor criticidad. En el primero de los casos nos encontraríamos con sectores como la energía, el transporte, las infraestructuras digitales y servicios tecnológicos, o con la propia industria nuclear; y en el segundo de los casos con los servicios postales y de mensajería, la gestión de residuos, los proveedores de servicios digitales o la seguridad privada. En cada una de las entidades se

23. https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2025/20250114-referencia-rueda-de-prensa-ministros.aspx (fecha de última consulta: 15/04/2025).


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

exige la existencia de una figura de interés, similar a la del delegado de protección de datos prevista en la Ley Orgánica 3/2018, de 5 de diciembre —si se nos permite el símil—, denominada "responsable de la seguridad de la información", que, entre sus funciones, tendrá las de diseñar la estrategia de protección, supervisar la implantación de medidas y garantizar el cumplimiento normativo, como desarrolla el artículo 16 del Anteproyecto, que, además, concreta que esta responsabilidad podrá ser asumida por una persona, una unidad o un órgano colegiado. Con todo, no se trata de una figura creada ex novo, sino que ya su origen radica en el artículo 7 del Real Decreto 43/2021.

Entre otras cuestiones, el Anteproyecto de Ley[24] prevé la creación de un nuevo organismo, denominado Centro Nacional de Ciberseguridad, que pasaría a engrosar la lista de organismos con competencias en esta materia[25] y que desgranamos *ut infra*[26], y que, tal y como reza el apartado III de la exposición de motivos de la norma, se constituye como la autoridad nacional competente única en la materia para la dirección, impulso y coordinación de todas las actividades previstas en dicha ley, erigiéndose en el punto de contacto único para garantizar la cooperación intersectorial y transfronteriza[27] con otras autoridades competentes, así como autoridad nacional de gestión de crisis de ciberseguridad, como recoge el artículo 6 del anteproyecto ahora analizado. De hecho, dicho centro, en su faceta de autoridad nacional de gestión de crisis de ciberseguridad, será responsable de la coordinación para la gestión de incidentes y crisis de ciberseguridad a gran escala, y a él se encomienda la adopción de un plan de respuesta a dichos incidentes, en el que se fijen los objetivos y las medidas a desarrollar[28].

24. Cuyo texto está disponible en el siguiente enlace: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf (fecha de última consulta: 18/04/2025).

25. Entre otros, como indica Pérez-Bes, el Mando Conjunto del Ciberespacio, el INCIBE, el Centro Criptológico Nacional, el CNPIC, el CNI o el Departamento de Seguridad Nacional (DSN), además de los correspondientes CERT de los tres primeros, y de los equipos especializados de las Fuerzas y Cuerpos de Seguridad del Estado, de la Fiscalía, o del Embajador en misión especial para las amenazas híbridas y la ciberseguridad, por citar algunos. Todo ello sin contar con el Consejo Nacional de Ciberseguridad. Esta información se puede consultar en el siguiente enlace: https://www.democrata.es/analisis-y-opinion/espana-contara-con-un-nuevo-centro-nacional-de-ciberseguridad/ (fecha de última consulta: 19/04/2025).

26. En el apartado 4 de este capítulo.

27. Prevista en el artículo 34 del anteproyecto en correlación con la previsión de asistencia mutua del artículo 37 de la directiva.

28. Pendiente, todo ello, de su desarrollo reglamentario.


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

En el ámbito de la Unión Europea, los organigramas son dispares entre sí y, de hecho, solo 13 de los Estados miembros cuentan con una única autoridad nacional de ciberseguridad, pese a que la Agencia de la Unión Europea para la Ciberseguridad, en su documento de 2023, "Un marco de gobernanza para las estrategias nacionales de ciberseguridad", recomienda contar con un organismo que supervise el cumplimiento de las entidades reguladas con las normas europeas e internacionales —además de dotar a las autoridades concernidas de competencia sancionadora— (Adeva y Vera, 2024: 99). En España, la posible creación de un organismo especializado en esta materia ha sido una posibilidad que se había barajado en otras ocasiones; sin embargo, la cuestión estriba en la definición que se haga de los objetivos, competencias y facultades del mismo, pues lo contrario sería aumentar el caos organizativo y generar duplicidades. Por eso también resulta de interés analizar si el centro ahora propuesto absorberá competencias ejecutivas, o se limitará a la mera supervisión.

En definitiva, aunque es pronto para fijar el impacto de la norma que transpondrá la Directiva (UE) 2022/2555, podemos aventurar la relevancia de dotar al futuro Centro Nacional de Ciberseguridad con la misión de dirigir, impulsar y coordinar las acciones relacionadas con la ciberseguridad, porque ello permitirá garantizar la cooperación intersectorial y transfronteriza por la que ya apostaba la directiva NIS aprobada en el año 2016. Sin embargo, en torno a la creación de este centro surgen numerosas incógnitas, pues existe el riesgo de que engrose la ya extensa lista de órganos con competencias en la materia en España, sin que se consiga una verdadera coordinación, pues el anteproyecto tampoco aclara, sobremanera, la cuestión competencial.

Finalmente, huelga destacar la mayor precisión respecto a la norma que transpuso la Directiva NIS 1 en lo que a la notificación de incidentes se refiere, y un régimen sancionador (artículos 36 y siguientes) más detallado que incluye sanciones proporcionales y disuasorias (acompañadas de otras medidas correctivas —como las auditorías de seguridad—), que pueden oscilar entre los 10 millones de euros y un máximo de un 2 % del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior.

No debemos olvidar, por cierto, que el "Informe de 2024 sobre el estado de la ciberseguridad en la Unión", citado en el epígrafe introductorio de este capítulo, es fruto de la propia Directiva NIS 2, que en su artículo 18 conmina a la ENISA a adoptar "un informe bienal sobre la situación de la


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

ciberseguridad en la Unión", con su correspondiente remisión y presentación en el Parlamento Europeo.

## 3. La relevancia de la ciberseguridad en el ámbito de la seguridad nacional y de las Administraciones públicas

La creciente digitalización de las sociedades actuales ha traído consigo no solo avances en lo que a eficiencia, conectividad e innovación se refiere, sino también una dependencia crítica de las infraestructuras tecnológicas que soportan los servicios esenciales. En este contexto, la ciberseguridad ha dejado de ser un ámbito meramente técnico para convertirse en una cuestión estratégica que afecta de lleno a la seguridad nacional, como ya se ha dejado entrever al inicio de este capítulo. De hecho, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, cita de forma expresa entre los ámbitos de especial interés de la propia seguridad nacional[29] —previstos en su artículo 10— a la ciberseguridad. Conviene destacar a este respecto, por cierto, que la ciberseguridad está plenamente interconectada con el resto de ámbitos de especial interés previstos en dicho artículo, como la seguridad energética, que cuenta con documentos de análisis propios, tales como la Estrategia de Seguridad Energética Nacional, que hace referencia a la ciberseguridad en varias ocasiones y que debe ser actualizada —pues, tal y como se pudo comprobar con el apagón energético del pasado 28 de abril de 2025, una estrategia que data del año 2015[30], como es esta, no es operativa en la actualidad—.

En el ámbito de las ciberamenazas, son frecuentes los ataques de potencias extranjeras consideradas hostiles por nuestros servicios de inteligencia, como Rusia, cuyos ataques pretenden socavar nuestro Estado de derecho. Sin ir más lejos, a comienzos del mes de marzo del año 2025, las diputaciones de Badajoz y Cáceres y varios ayuntamientos españoles, entre los que se encontraban los de A Coruña, Vigo, Lugo, Santiago, Murcia, Palma o Mérida, sufrieron varios ataques que provenían de *hackers* rusos, cuyo principal objetivo era colapsar los servidores para acceder a las correspondientes sedes electrónicas, por la ingente cantidad de datos que albergan concernientes a los ciudadanos de dichos municipios. Las ofensivas fueron perpetradas, presuntamente, por el grupo de *hackers*

29. En palabras de la propia norma, estos son todos aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales.

30. Su contenido está disponible en el siguiente enlace: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/ESTRATEGIA%20DE%20SEGURIDAD%20ENERG%C3%89TICA%20NACIONAL%20(WEB).pdf (fecha de última consulta: 18/05/2025).

prorruso "NoName057", que ya había atacado durante el año 2024 al poder legislativo de la Comunidad Autónoma de Galicia[31].

La protección de las redes y sistemas de información forma hoy parte del núcleo duro de las políticas de defensa y seguridad de los Estados, entre ellos España. La Estrategia de Seguridad Nacional de 2013 fue la primera en reconocer expresamente a la ciberseguridad como una dimensión fundamental de la seguridad del Estado, al señalarla como una de las principales amenazas del entorno actual. Desde entonces, la inclusión de este ámbito en las estrategias y normas de seguridad nacional se ha ido consolidando hasta el punto de que, *hoc die*, resulta impensable una concepción de la seguridad nacional desligada de la dimensión cibernética.

Sin embargo, como ya hemos adelantado en el apartado introductorio de este capítulo, no debemos hacer descansar el concepto de "ciberseguridad" única y exclusivamente en el ámbito de la lucha contra las ciberamenazas. Pues una visión reduccionista del fenómeno, relegando dicho concepto a la respuesta técnica frente a los ciberataques —en sus múltiples formas—, dejaría fuera de órbita a gran parte del alcance y complejidad estratégica del concepto. La ciberseguridad no se limita, por tanto, a repeler amenazas externas, sino que constituye, en realidad, un sistema integral de garantías orientado a preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información digital y de los sistemas que la gestionan. Ergo, la ciberseguridad, ligada al concepto de seguridad nacional y a las normas que lo cercan, se erige como una estrategia de seguridad institucional, jurídica, organizativa y cultural, que abarca desde los *firewalls* hasta la formación de empleados, desde la gestión de contraseñas hasta la redacción de protocolos legales de respuesta, y desde la vigilancia tecnológica hasta la protección de la confianza ciudadana. En esos términos se pronuncia el Informe Anual de Actividad de la Agencia Vasca de Ciberseguridad (2024: 14), que insiste en que "hay que tener presente que la ciberseguridad no es solo una cuestión técnica, sino también responsabilidad ética y social, ya que afecta a la protección de los datos personales, al ejercicio de la ciudadanía de sus derechos y a la prestación de servicios públicos esenciales".

Este enfoque se ha materializado en un conjunto articulado de normas, estrategias y planes que parten del núcleo normativo de la Ley de

31. A este grupo se hace referencia en la página 14 del informe anual de actividad —correspondiente al año 2024— de la Agencia Vasca de Ciberseguridad, denominada Cyberzaintza, que está disponible en el siguiente enlace: https://ciberseguridad.euskadi.eus/media/web-cyb00-Memoria2024_Cyberzaintza.pdf (fecha de última consulta: 15/04/2025).


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

Seguridad Nacional —que desarrollaremos en el siguiente subepígrafe—, y se despliegan a través de instrumentos como la Estrategia de Seguridad Nacional, el Esquema Nacional de Seguridad o el reciente Plan Nacional de Ciberseguridad. Todos estos instrumentos contribuyen a construir un modelo organizativo y normativo de protección del entorno digital, en donde las Administraciones públicas —incluidas las entidades locales— asumen un papel activo y coordinado en la defensa de los intereses generales en el ciberespacio.

Aunque en los siguientes subepígrafes se reflexionará sobre cada uno de los instrumentos ahora citados, huelga identificarlos de forma sucinta antes de comentar el análisis detallado de los mismos[32]. En primera instancia, la Ley de Seguridad Nacional es una ley orgánica —del año 2015— que establece el marco legal general de la seguridad nacional. En segundo término, la Estrategia de Seguridad Nacional —del año 2021— es un documento estratégico que define amenazas y prioridades y ofrece una serie de directrices no vinculantes, a diferencia del Esquema Nacional de Seguridad —del año 2022—, que es un reglamento técnico[33] que establece medidas mínimas en el ámbito de la ciberseguridad vinculante para todas las Administraciones públicas. En tercer y último lugar, el Plan Nacional de Ciberseguridad —del año 2022— es un plan de acción del Ejecutivo, o lo que es lo mismo, la estrategia a seguir para la mejora y refuerzo de la ciberseguridad de infraestructuras críticas, Administraciones y actores privados, que desarrolla la Estrategia Nacional de Ciberseguridad.

Todos ellos toman como base el superior interés nacional que requiere mejorar la coordinación de las diferentes Administraciones públicas y, por ende, fomentar la acción conjunta de los agentes e instrumentos al servicio de la propia seguridad nacional, como veremos a continuación.

### 3.1. La Ley de Seguridad Nacional y la Estrategia de Seguridad Nacional

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, constituye el pilar normativo fundamental en la materia. Se trata de una ley orgánica que regula el funcionamiento del Sistema de Seguridad Nacional, entendido como el conjunto coordinado de órganos, medios y procedimientos

32. Un análisis de los documentos y textos normativos más relevantes en el ámbito de la ciberseguridad en relación con la Seguridad Nacional puede encontrarse en el documento "Ámbitos de la Seguridad Nacional: Ciberseguridad", disponible en el siguiente enlace: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=397_Ambitos_de_la_Seguridad_Nacional_Ciberseguridad&modo=2 (fecha de última consulta: 15/04/2025).

33. El vigente se halla regulado en el Real Decreto 311/2022.


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

destinados a garantizar la seguridad del Estado frente a amenazas y riesgos diversos. Así pues, esta tiene por objeto regular los principios básicos, los órganos superiores y autoridades, y los componentes fundamentales de la Seguridad Nacional; el Sistema de Seguridad Nacional, su dirección, organización y coordinación; la gestión de crisis, y la contribución de recursos a la Seguridad Nacional.

Como ya se ha resaltado *ut supra*, esta ley incluye expresamente a la ciberseguridad como uno de los ámbitos de especial interés en el artículo 10, lo que no es una cuestión baladí.

Uno de los instrumentos clave de esta ley es la "situación de interés para la Seguridad Nacional", un concepto intermedio entre la normalidad y los estados previstos por el artículo 116 de la Constitución Española (alarma, excepción y sitio) y regulados por la Ley Orgánica 4/1981, de 1 de junio. Esta situación, regulada en los artículos 23 y siguientes de la Ley Orgánica 36/2015, permite al Gobierno adoptar medidas extraordinarias para hacer frente a crisis que afecten a la seguridad nacional[34] sin necesidad de recurrir a la declaración de uno de los regímenes de excepción previstos constitucionalmente.

La norma prevé que, en tales supuestos, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, se produzca la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, también desde el punto de vista territorial, pues el artículo 22 exige la participación de "las autoridades de la Comunidad Autónoma que, en su caso, resulte afectada", en la gestión de la crisis. Esta previsión es especialmente relevante en escenarios de ciberataques masivos, ataques híbridos o interrupciones críticas de servicios digitales clave, y es una muestra de una de las características esenciales del modelo español y europeo de protección de infraestructuras críticas: la colaboración —también público-privada— estructurada.

En consonancia con lo anterior, apuntamos que la mayoría de las infraestructuras críticas no están gestionadas por el Estado, sino por grandes empresas privadas o por operadores mixtos. Por tanto, la seguridad nacional depende en gran medida de la seguridad de actores privados. Esto obliga a establecer mecanismos de cooperación estables, eficaces y protegidos legalmente. De hecho, tal y como recoge el Código de Buen

34. Que en ningún caso podrá implicar la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos.


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

Gobierno de la Ciberseguridad (2023: 7), "en abril del año 2019, el Consejo de Seguridad Nacional aprobó la Estrategia Nacional de Ciberseguridad en cuyo texto se destaca la cooperación público-privada como un elemento clave en la consecución de los objetivos marcados en ciberseguridad".

Otro aspecto de interés de la Ley de Seguridad Nacional es que establece el Consejo de Seguridad Nacional[35] como órgano colegiado de máximo nivel en la materia, al que corresponde asistir al jefe del Ejecutivo en la dirección de la política de seguridad nacional y del Sistema de Seguridad Nacional, y, entre sus funciones principales, tiene la de elaborar la Estrategia de Seguridad Nacional, que es el documento rector de la política pública en este campo —y que, como veremos a continuación, tiene una especial relevancia para la planificación de la ciberseguridad en el marco estatal—, o dirigir y coordinar las actuaciones de gestión de situaciones de crisis, tal y como ocurrió el pasado 28 de abril de 2025 con el apagón eléctrico masivo que afectó a España. Esta situación provocó que en un margen temporal de tres días el Consejo de Seguridad Nacional se reuniese en seis ocasiones[36].

Además, el artículo 20 de la Ley 36/2015 establece que las capacidades de ciberseguridad del Estado forman parte de las estratégicas del Sistema de Seguridad Nacional, junto con otras como las capacidades militares, las de inteligencia o las de protección civil. Esta equiparación refleja claramente la importancia creciente de la dimensión digital en la arquitectura de seguridad.

Por otro lado, la Estrategia de Seguridad Nacional[37] es el documento marco de la política de seguridad del Estado[38], que se encuentra vigente desde el 28 de diciembre del 2021, en sustitución de la anterior, publicada en 2017. Esta constituye una visión integral, prospectiva y adaptativa de los riesgos y amenazas que afectan a España, lo que se manifiesta, también, a través de su proceso de elaboración, que, aunque recae en el

35. Es la pieza angular del Sistema de Seguridad Nacional y es el órgano responsable de la dirección y la coordinación de las actuaciones para la gestión de situaciones de crisis, como reconoce el capítulo V del Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

36. A este respecto, puede consultarse el contenido publicado de alguna de esas reuniones en el siguiente enlace: https://www.dsn.gob.es/estructuras-de-seguridad-nacional/el-consejo-de-seguridad-nacional (fecha de última consulta: 18/05/2025).

37. Sobre los orígenes de las Estrategias de Seguridad Nacional puede resultar interesante la consulta de Blesa López (2018).

38. Tal y como define el artículo 4 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.


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

Consejo de Seguridad Nacional[39] —como ya se ha adelantado—, cuenta con la participación de las comunidades y de las ciudades autónomas a través de la Conferencia Sectorial para Asuntos de Seguridad Nacional. También tiene en cuenta las aportaciones de expertos independientes, personas de reconocido prestigio, conocimientos y experiencia en el campo de la seguridad.

En la Estrategia de Seguridad Nacional del año 2021, la ciberseguridad es identificada como una prioridad de organizaciones y Gobiernos[40], en tanto en cuanto los ataques cibernéticos son cada vez más frecuentes, sofisticados y disruptivos, con capacidad para afectar no solo a la economía o a la privacidad de los ciudadanos, sino también a la soberanía, la defensa y la estabilidad institucional del país. Se advierte expresamente del riesgo de ciberataques provenientes de Estados hostiles —o incluso de grupos terroristas—, cuya actividad ha dejado de seguir cánones tradicionales para involucrar las llamadas estrategias híbridas, en las que la seguridad de la red, o del ciberespacio, juega un papel primordial.

Este documento cuenta con tres ejes estratégicos[41] sobre los que se articulan una serie de líneas de acción, en cumplimiento del mandato del artículo 4.2 de la Ley Orgánica de Seguridad Nacional. Entre estas líneas de acción, y en estricta relación con la ciberseguridad, destacan el refuerzo de la ciberdefensa, integrando capacidades civiles y militares; la consolidación de una arquitectura de gobernanza de la ciberseguridad, con funciones claras, mecanismos de cooperación y protocolos de respuesta; el fomento de una cultura de ciberseguridad en todos los niveles sociales, incluyendo el sistema educativo, el sector empresarial y la Administración pública; o la protección de las infraestructuras críticas digitales, como garantía de la continuidad de los servicios esenciales.

De hecho, se incorpora el concepto de "ciberespacio" como uno de los espacios comunes globales sobre los que "resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía", como reconoce el propio documento en su capítulo IV. De ahí que se convierta en una prioridad garantizar su uso

39. Anótese que la coordinación del proceso ha sido llevada a cabo por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.

40. Como reza el capítulo I en su apartado "transformación digital".

41. Como reconoce el capítulo IV de la misma, titulado "un planeamiento estratégico integrado", los tres ejes son: una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional; una España que promueve la prosperidad y el bienestar de los ciudadanos; y una España que participa en la preservación de la paz y la seguridad internacional y defiende sus intereses estratégicos.


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

fiable y seguro, "a fin de proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico". En conexión con lo anterior, en el marco del impulso a la dimensión preventiva del Sistema Nacional de Protección de las Infraestructuras Críticas, se realiza un "especial énfasis en la protección de los sistemas informáticos de las Infraestructuras Críticas y operadores de servicios esenciales frente a ciberamenazas", otorgando un papel relevante a la colaboración público-privada y al I+D+i a efectos de robustecer la resiliencia frente a los ciberataques.

En este concepto, el de "resiliencia" —entendido como la capacidad del país para anticiparse, resistir, recuperarse y adaptarse frente a situaciones de crisis, incluyendo las originadas en el ciberespacio, y que incluye la progresión desde una situación de normalidad hasta la recuperación después de una situación de crisis—, la Estrategia también propone la integración de la ciberseguridad. Así pues, en el seno del V capítulo, dedicado a la gestión de crisis en el marco del Sistema de Seguridad Nacional, en donde el principio de resiliencia tiene un protagonismo inequívoco, la cuarta de las actuaciones concretas que se prevén exige la integración de la información de la Seguridad Nacional a través de soluciones tecnológicas.

De nuevo, aparece de forma protagonista el principio de colaboración entre Administraciones y de estas con otros sectores de la sociedad, en tanto en cuanto "el concepto de resiliencia supone una integración multinivel en el modelo de gestión de crisis, que incorpora tanto la coordinación entre todas las Administraciones públicas (estatal, autonómica y local), como entre los ministerios, el sector privado y científico y la sociedad civil", como reconoce el capítulo V de la Estrategia. Esta necesidad de cooperación se vuelve de especial trascendencia en el marco de estrategias híbridas, dado el carácter multidimensional y coordinado de este tipo de amenazas, que persiguen atentar contra la estabilidad de los Estados y las instituciones[42]. La necesidad de una respuesta amplia y multinivel está presente, por cierto, en la Unión Europea desde principios del siglo XX; como ejemplo, la existencia de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) —ya citada—, que es la agencia de la Unión que, desde el año 2004, se ha dedicado a lograr un alto nivel común de ciberseguridad en toda Europa[43].

42. Como reconoce el propio capítulo V de la Estrategia de Seguridad Nacional del año 2021 en el apartado "Enfoque integral que garantice la resiliencia".

43. Su web está disponible en el siguiente enlace: https://www.enisa.europa.eu/about-enisa/who-we-are (fecha de última consulta: 19/04/2025).


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

### 3.2. El Esquema Nacional de Seguridad. Su posible incidencia en la Administración local

El Esquema Nacional de Seguridad, regulado actualmente por el Real Decreto 311/2022, es una norma jurídica específica cuyo objetivo es establecer los principios básicos y requisitos mínimos que deben cumplir las Administraciones públicas y los proveedores de servicios del sector privado que gestionan información o prestan servicios a las entidades del sector público, como indica el artículo 2 del ya citado real decreto en su párrafo primero y tercero. Es, por tanto, un instrumento clave para garantizar la seguridad de los sistemas de información del sector público, que debe considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional, recogidos en la Ley 36/2015[44], ya analizada *ut supra*.

A modo de introducción: el Esquema Nacional de Seguridad, que tiene su origen en el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fue actualizado mediante el Real Decreto 951/2015, de 23 de octubre, a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Sin embargo, su última actualización ha venido, como detallaremos en este epígrafe y acabamos de adelantar, de la mano del Real Decreto 311/2022, que adaptó dicho esquema a las nuevas exigencias normativas (como el Reglamento General de Protección de Datos o la propia Directiva NIS), con la finalidad de incorporar mejores prácticas internacionales y de responder a los nuevos desafíos del entorno digital —como el uso de la nube, el teletrabajo o la inteligencia artificial—. Entre las novedades destacan la introducción del principio de vigilancia continua —regulado en el artículo 10—, la gestión basada en el ciclo de vida de los sistemas —citado, entre otros, en el artículo 36— y la obligatoriedad de notificar incidentes que tengan un impacto significativo —artículo 33.2 y 33.7—.

El Esquema Nacional de Seguridad se basa en siete principios fundamentales: la gestión de la seguridad basada en los riesgos; la prevención,

44. Como reconoce el artículo 1 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.


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

detección, respuesta y conservación; la existencia de líneas de defensa; la vigilancia continua; la reevaluación periódica; la diferenciación de responsabilidades y, en especial, la seguridad como proceso integral. Ergo, el concepto de seguridad está constituido, en virtud del artículo 6 del Real Decreto, por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, lo que excluye, *de facto*, cualquier actuación puntual o tratamiento coyuntural.

Una de las principales fortalezas del Esquema Nacional de Seguridad es su capacidad de homogeneizar los requisitos de seguridad en todas las Administraciones públicas[45], evitando la fragmentación normativa y técnica. Asimismo, facilita la contratación de servicios TIC con garantías mínimas, ya que obliga a los proveedores tecnológicos a cumplir los estándares establecidos, y presta especial atención a las necesidades de la Administración local. Así, su artículo 12.5 prevé la posibilidad de que los municipios dispongan de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales. Sin embargo, lo habitual es que cada ayuntamiento, por estar incluido en el ámbito de aplicación del Real Decreto, según su artículo 2, disponga de la suya. Como ejemplo, la política de seguridad del Ayuntamiento de Frades, en A Coruña, aprobada en el año 2023[46], que respeta cada una de las exigencias del artículo 12 del Real Decreto, relativa a la política de seguridad y requisitos mínimos de seguridad, y que prevé que la figura de responsable de la información recaiga en el alcalde-presidente, salvo delegación en la concejalía que corresponda. Otro ejemplo lo encontramos, también en la provincia de A Coruña, en el Ayuntamiento de Cariño[47], que constituye un comité de seguridad integrado por varios miembros en donde se designa responsable de la seguridad a la persona que ostenta la secretaría municipal. También en el ámbito local, la Diputación de la provincia de A Coruña cuenta, por mandato legal, con una política de seguridad de la información —revisada en marzo de 2022[48]— en donde se designa

45. Artículo 12 del Real Decreto 311/2022.

46. Disponible en el siguiente enlace: https://sede.frades.gal/sxc/export/sites/frades/recursos/downloads/Normativa/Certificado-ac-pleno-politca-ciberseguridade.pdf (fecha de última consulta: 20/04/2025).

47. Disponible en el siguiente enlace: https://bop.dacoruna.gal/bopportal/publicado/2023/12/12/2023_0000009673.pdf (fecha de última consulta: 17/04/2025).

48. Tal y como se puede corroborar en el siguiente enlace: https://sede.dacoruna.gal/sxc/export/sites/diputacion/recursos/downloads/Normativa/Politica_de_Seguridad_aprobada_25.03.22.pdf. Por su lado, la política de seguridad de la información de la Administración general y del sector público autonómico de Galicia fue publicada junto con la política de protección de datos personales en la Resolución de 22 de octubre de 2024 del Diario Oficial de Ga-


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

responsable de la seguridad de la información a la persona que ostente la jefatura del Servicio de Informática y Administración Electrónica, y en donde se designa presidente del Comité de Seguridad a la persona que ostente la presidencia del órgano de gobierno de la provincia.

Como crítica, más allá de aquellas disposiciones en donde se designa a los responsables y se concretan las funciones de cada actor, las políticas de seguridad se han convertido en meros documentos programáticos reiterativos respecto del Esquema Nacional de Seguridad que no aportan gran valor, *de facto*, a la creación de un entorno nítido de seguridad o frente a amenazas reales en el ámbito de las Administraciones públicas. Sin embargo, su cumplimiento es obligatorio, y su verificación puede realizarse mediante auditorías periódicas internas o externas, en consonancia con la previsión del artículo 31 del Real Decreto. El Esquema Nacional de Seguridad, por cierto, tiene incidencia, incluso, en el ámbito de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) —concepto que, a nuestros efectos, debemos entender *lato sensu*—. Pues, como ejemplo, una gran cantidad de ayuntamientos a nivel estatal emplean Intelcops[49], un *software* que simplifica la operativa diaria de la gestión policial, desde las gestiones administrativas, las relativas a delitos y sanciones, atestados e informes, hasta la gestión interna y de recursos humanos, y que está adaptado al propio Esquema Nacional de Seguridad y a los requisitos y condicionantes en él establecidos.

### 3.3. El Plan Nacional de Ciberseguridad y otros documentos de interés

El Plan Nacional de Ciberseguridad es el instrumento operativo que materializa los objetivos estratégicos fijados en la Estrategia de Seguridad Nacional. Fue aprobado en marzo de 2022, en un contexto marcado por el conflicto bélico en Ucrania, por el aumento de ciberataques contra infraestructuras críticas europeas y por una creciente tensión geopolítica en el ciberespacio[50]. Su contenido es de alcance limitado y con su aproba-

licia, disponible en el siguiente enlace: https://www.xunta.gal/dog/Publicados/2024/20241113/AnuncioG0177-041124-0001_es.html (fecha de última consulta de ambos enlaces: 17/04/2025).

49. Otro de los *softwares* más empleados es Appolo, que permite realizar un seguimiento de la actividad de los agentes, la tramitación electrónica de documentos y expedientes, la conexión con la Dirección General de Tráfico y otros servicios públicos.

50. Huelga señalar la creación del *NATO Integrated Cyber Defence Centre*, anunciado en el año 2024, a fin de que los aliados que integran la Alianza Atlántica puedan superponerse de mejor forma, e incluso anticiparse, a los ataques cibernéticos. A este respecto, se puede consultar el comunicado oficial de la OTAN en el siguiente enlace: https://www.nato.int/cps/en/natohq/news_227647.htm.


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

ción se da cumplimiento, por tanto, al mandato emitido por el Consejo de Seguridad Nacional.

Sobre el alcance limitado de su contenido resulta de interés consultar la respuesta del Gobierno ante la pregunta de varios diputados del Grupo Parlamentario de VOX en el Congreso de los Diputados[51] sobre la publicidad del plan que ahora analizamos. Su libre difusión, afirma el Ejecutivo, podría comprometer la estructura de ciberseguridad de España por parte de actores hostiles, motivo que justifica su publicación parcial y, en todo caso, de medidas concretas sobre las que ya existía algún tipo de información pública previa.

Así pues, entre los pocos datos que se han ofrecido sobre este plan, sabemos que se articula sobre un total de 150 medidas distribuidas en siete ejes estratégicos[52], que abarcan desde la mejora de la capacidad nacional de prevención, detección y respuesta, hasta el fomento del talento, la concienciación ciudadana o la cooperación internacional. Además, el Plan Nacional de Ciberseguridad responde a una integración de esfuerzos fruto de la naturaleza transversal y polimórfica de las amenazas cibernéticas, que no respetan fronteras, horarios ni jurisdicciones. O lo que es lo mismo, el principio de colaboración vuelve a cobrar especial importancia, pues las medidas previstas según las directrices del plan se ejecutarán bajo la coordinación del Departamento de Seguridad Nacional, y su examen se articulará a partir de indicadores de cumplimiento y de mecanismos de revisión periódica sobre los diferentes organismos que participarán en su ejecución. En este último sentido, reconoce la nota de prensa del Consejo de Ministros de 29 de marzo de 2022[53] que "el Plan prevé la creación de un sistema de seguimiento y control, con el fin de poder identificar el grado de ejecución de las medidas y emitir un informe anual de evaluación".

De forma pareja a la aprobación del Plan Nacional de Ciberseguridad se produjo la aprobación del Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, cuyo objetivo princi-

51. Disponible en el siguiente enlace: https://www.congreso.es/entradap/l14p/e24/e_0240255_n_000.pdf (fecha de última consulta: 12/04/2025).

52. Y que está dotado con un presupuesto de mil millones de euros.

53. Disponible en el siguiente enlace: https://www.mpr.gob.es/prencom/notas/paginas/2022/290322-ciberseguridad.aspx, o, de forma más amplia, en https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad (fecha de última consulta de ambos enlaces: 09/03/2025).

pal es fortalecer el ámbito de la ciberseguridad e impulsar una seguridad integral en el contexto del ecosistema generado por la tecnología 5G. Ello, en el escenario del conflicto internacional derivado de la agresión contra Ucrania, pues, a la luz de los acontecimientos acaecidos en aquel entonces, desde las instituciones europeas se observaba como elevado el riesgo de ciberataques contra redes y servicios 5G ya desplegados en nuestro país o con despliegue previsto para los próximos meses[54]. Sobre este real decreto, analizaremos diferentes cuestiones en el siguiente subepígrafe.

Es importante resaltar, en último lugar, que la amalgama de documentos existentes en materia de ciberseguridad, especialmente en relación con el elemento de la seguridad nacional, es extensa. En este capítulo se abordan, directamente, aquellos que por su ámbito de aplicación material o subjetivo son de mayor interés, pero existen otros muchos de incidencia menor que pueden tener algún tipo de afectación sobre la materia objeto de estudio en este libro colectivo.

A modo de ejemplo, la Estrategia de Seguridad Nacional del año 2017 establecía en su capítulo V la necesidad de aprobar un Plan Integral de Cultura de Seguridad Nacional que sirviera de catalizador para la implantación progresiva de una cultura de seguridad nacional inclusiva, participativa y colaborativa, todo ello con el fin de reforzar el Sistema de Seguridad Nacional, mejorar la coordinación y eficacia de la acción del Estado y la participación de la sociedad, tal y como reza el anejo de la Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba, precisamente, dicho Plan Integral de Cultura de Seguridad Nacional[55]. Este plan es citado, también, en la nueva Estrategia de Seguridad Nacional, que en su capítulo IV, relativo al planteamiento estratégico integrado, recoge la necesidad de implementar las acciones incluidas en el Plan Integral de Cultura de Seguridad Nacional, para lo que contempla como elemental el principio de colaboración entre las diferentes Administraciones públicas, con la connivencia del sector privado y de la sociedad civil.

54. De nuevo, la ciberseguridad demuestra la relevancia de su componente geopolítico. De hecho, en este caso, esta es la circunstancia que el Gobierno utilizaba para justificar la concurrencia de las razones de extraordinaria y urgente necesidad exigidas por el artículo 86 de la Constitución Española para la tramitación de la norma como un decreto-ley.

55. Este está disponible en el siguiente enlace: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-9631 (fecha de última consulta: 07/04/2025).


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

También existen otros documentos interesantes[56], especialmente en el ámbito del estudio de las cuestiones geopolíticas, como el Plan Integral de Seguridad para Ceuta y Melilla, citado en la propia Estrategia —en la línea de acción número 12—, en donde cobra especial relevancia el ámbito del ciberespacio y la mejora de las capacidades tecnológicas de nuestro país, pues las amenazas híbridas adquieren mayor relevancia por su capacidad de desestabilizar las instituciones del Estado y por su impacto sobre la vida y libertad de los ciudadanos.

Destacamos, finalmente, el Plan de Digitalización de las Administraciones Públicas 2021-2025[57], que, en su medida 17, se preocupa de la transformación digital de las comunidades autónomas y de las entidades locales, aunque, fundamentalmente, el apoyo a estas se centrará en la ayuda financiera para la realización de proyectos vinculados con la transformación digital, como la implementación del teletrabajo o la automatización de procesos, y no en el ámbito de la ciberseguridad. Este hecho, entendemos, es una oportunidad perdida. Pues no se puede plantear un avance en la digitalización de las corporaciones locales si estas no cuentan con la estructura de protección necesaria, ni con las capacidades de respuestas ante incidentes, ya que, de este modo, lo que se favorece es la interdependencia de la tecnología, que, en caso de producción de un incidente, dejaría a los ayuntamientos en una situación de mayor vulnerabilidad. No es menos cierto que dicho plan sí que destina una serie de apartados específicos a abordar el fenómeno de la seguridad en el ciberespacio —por ejemplo, en el apartado 9.3—, pero no concreta medidas en favor de las Administraciones locales, pese a que sus particularidades y sus menores capacidades en este ámbito así lo justifican.

### 3.4. La Administración pública y las infraestructuras críticas: especial atención a la Ley 8/2011 y a su reglamento de desarrollo

La protección de las infraestructuras críticas constituye uno de los ejes vertebrales de la política de ciberseguridad de cualquier Estado moderno. En un mundo cada vez más interconectado y digitalizado, donde los servicios esenciales —como la electricidad, el agua, el transporte, la sani-

56. No solo nos encontramos en este ámbito documentos jurídicos, sino también otros jurídicamente no vinculantes, como el Código de Buen Gobierno de la Ciberseguridad, ya citado anteriormente.

57. Al que se puede acceder en el siguiente enlace: https://administracionelectronica.gob.es/pae_Home/en/pae_Estrategias/Plan_Digitalizacion_AAPP.html?urlMagnolia=/pae_Home/en/pae_Estrategias/Estrategia-TIC/Plan-Digitalizacion-AAPP.html (fecha de última consulta: 09/05/2025).


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

dad o las telecomunicaciones— dependen en gran medida de sistemas informáticos, los ciberataques contra estas infraestructuras pueden tener consecuencias devastadoras para la seguridad nacional, la economía y el bienestar de los ciudadanos. De hecho, uno de los retos más complejos a los que la seguridad nacional se enfrenta es la sofisticación y frecuencia creciente de los ciberataques, que "no solo están dirigidos a entidades gubernamentales, sino también a infraestructuras críticas como redes eléctricas, sistemas financieros, servicios de salud y redes de telecomunicaciones" (Rodríguez González, 2024).

A nivel internacional, los ciberataques contra infraestructuras críticas han demostrado su capacidad disruptiva en diversas ocasiones. El caso más paradigmático fue el del *ransomware WannaCry* en 2017, que afectó a más de 300 mil equipos en todo el mundo, incluyendo hospitales del sistema de salud británico y a empresas estratégicas como Telefónica. Ya en territorio nacional, pocos organismos públicos han sido ajenos a esta tendencia: desde el Servicio Andaluz de Salud[58] o las corporaciones locales, como indicamos al comienzo de este capítulo, hasta la Agencia Estatal de Administración Tributaria o el propio Servicio Público de Empleo Estatal, en este último caso el 9 de marzo de 2021[59]. A comienzos del año 2025, se detectaron en la *dark web* datos personales —más de 160 mil— de miembros de las FCSE, que, según el Instituto Nacional de Ciberseguridad[60], podrían estar vinculados a un ataque de *ransomware* ocurrido en marzo de 2024 contra una empresa subcontratada para realizar reconocimientos médicos. Más recientemente, a finales de septiembre de 2025, otra filtración de datos de diferentes representantes públicos, entre los que se hallaban el presidente del Gobierno y diferentes ministros, provocaba que la Audiencia Nacional iniciase una investigación después de que la Comisaría General de Información (CGI) de la Policía Nacional entregara un informe en el que figuraba como responsable un *hacker* autodenominado "N4t0X".

En nuestro país, el marco legal, institucional y estratégico en materia de protección de infraestructuras críticas está íntimamente vinculado al desa-

58. Resulta interesante en este punto la lectura de Jareño y Arratibel (2024) sobre las recomendaciones de la Agencia Europea de Ciberseguridad ante incidentes de seguridad en el sector sanitario.

59. Se puede consultar más información sobre el incidente de seguridad en la página web del INCIBE, concretamente en el siguiente enlace: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/el-sepe-comienza-recuperar-sus-servicios-despues-sufrir (fecha de última consulta: 10/04/2025).

60. Como se puede comprobar en el siguiente enlace: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/detectados-datos-de-personales-supuestamente-de-la-guardia-civil-y-del (fecha de última consulta: 10/04/2025).


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

rrollo de la ciberseguridad como política pública. Desde hace más de una década España ha ido consolidando un modelo que articula la colaboración público-privada, la coordinación interadministrativa y la especialización operativa, en línea con las exigencias de la Unión Europea y los organismos internacionales de referencia, tal y como hemos reconocido líneas atrás.

Para comprender el verdadero alcance de la protección articulada en este ámbito —el de las infraestructuras críticas— debe resaltarse como uno de los rasgos distintivos de las amenazas modernas la convergencia entre el ámbito físico y el cibernético. Por eso, el enfoque actual de la protección de infraestructuras críticas exige una visión integral, en la que la ciberseguridad no sea una capa añadida, sino un elemento estructural.

La norma fundamental en esta materia es la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Esta ley parte del reconocimiento de que determinadas infraestructuras físicas y tecnológicas son esenciales para el funcionamiento normal de la sociedad, y de que su destrucción o interrupción podría generar consecuencias inasumibles. Por ello, impone a los operadores estratégicos una serie de obligaciones en materia de seguridad y planificación, aunque de forma limitada, en tanto en cuanto fue aprobada hace más de 15 años y, desde aquel entonces, la evolución de los elementos tecnológicos ha sido exponencial. A modo de ejemplo, a comienzos de la década pasada el concepto de inteligencia artificial resultaba ajeno y, *hoc die*, está presente en muchas de las facetas diarias de la vida de cualquier ciudadano. Pese a ello, podemos afirmar que la ciberseguridad aparece en esta ley como uno de los componentes fundamentales de la seguridad integral de las infraestructuras críticas, lo que no resta valor a nuestro argumento según el que existe la imperante necesidad de adecuar la norma al nuevo contexto.

En conexión con lo anterior, en cumplimiento del mandato previsto en la disposición final cuarta de la Ley, el Gobierno aprobó el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas[61], con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada ley. Pues bien, en dicho reglamento no se recoge en ninguna ocasión la palabra "ciberseguridad", lo que justifica, a nuestro juicio, su revisión.

Sea como fuere, la Ley define como infraestructura crítica, en su artículo 2, toda aquella que, siendo esencial, resulte indispensable y no susti-

61. En donde la Secretaría de Estado de Seguridad tiene un papel protagonista.


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

tuible a corto plazo, de forma que su perturbación tenga un gran impacto. Se establecen además los denominados operadores críticos, que son aquellas entidades u organismos responsables de la gestión de dichas infraestructuras —como se extrae del artículo 2 y del 13.2—. El artículo 4 de la norma contempla la existencia del Catálogo Nacional de Infraestructuras Estratégicas, que se erige como el instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país; es decir, el catálogo es el registro de carácter administrativo que tiene como finalidad la ágil disposición de una información completa, actualizada y contrastada sobre la totalidad de las infraestructuras estratégicas en el territorio nacional, incluidas las infraestructuras críticas, así como aquellas clasificadas como críticas europeas, que afecten a España. Sin embargo, de nuevo nos topamos con cierta opacidad, pues dada la alta sensibilidad de la información contenida en el Catálogo, se le confiere la calificación de secreto, como se puede extraer de la respuesta que el Gobierno da a una pregunta planteada por el Grupo Parlamentario Confederal de Unidas Podemos-En Comú Podem-Galicia en Común en abril del año 2022.

A los efectos de la temática en la que se ha orientado este libro colectivo es fundamental destacar el artículo 5 de la Ley 8/2011, porque prevé que las corporaciones locales sean agentes del Sistema de Protección de Infraestructuras Críticas, cuyas funciones se encuentran dispersas en el Reglamento ya citado. Entre otras, la custodia de los planes de apoyo operativo (artículo 31 del Reglamento) o la elaboración —siempre que sean agentes del Sistema los afectados— de los diferentes planes estratégicos sectoriales, en colaboración con el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (artículo 12 del Reglamento).

Como se observa, entre otros motivos, a partir de la previsión de la existencia de planes estratégicos sectoriales, el enfoque ligado a la particularidad de cada sector en la protección de infraestructuras críticas es una de las claves del modelo español. Entre otros, y a los efectos que aquí nos interesan, el Plan Sectorial de la Administración, que en aquel momento se constituía como el plan sectorial número 18 aprobado desde la constitución de la Comisión Nacional para la Protección de Infraestructuras Críticas (CNPIC)[62] —prevista en el artículo 11 de la Ley ahora analizada como órgano colegiado adscrito a la Secretaría de Estado de Seguridad—. Sus funciones, por cierto, también han sido desarrolladas reglamentariamente, pero, en este caso, sí que se encuentran perfectamente estructuradas en el artículo 11 del Real Decreto.

62. Que también es un agente del sistema, al igual que las corporaciones locales, como consecuencia de la previsión del artículo 5.2, letra g), de la Ley 8/2011.


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

Aunque no tenga relación estricta con el ámbito de la ciberseguridad, debe destacarse que estos planes, tal y como recoge el apartado web de la página oficial de la CNPIC[63], "permitieron que todas las entidades clave que debían intervenir en la lucha contra la pandemia ya estuvieran identificadas y perfectamente coordinadas cuando llegó la Covid-19", lo que permitió que los trabajadores esenciales "pudiesen continuar con la movilidad -tanto nacional como internacional- a pesar de las restricciones".

## 4. Entidades clave en materia de ciberseguridad en España

Una vez que hemos analizado la normativa que resulta de interés, conviene prestar especial atención a todos aquellos centros, organismos o agentes que intervienen de forma especializada en lo que a la protección de la ciberseguridad en España se refiere, los cuales constituyen un entramado organizativo de extrema complejidad frente a los modelos adoptados por otros países (Almeida Cerreda, 2025).

Además, debe entenderse su participación dentro de una estructura de coordinación interinstitucional mucho más amplia que involucra al Gobierno, a las comunidades autónomas y a las corporaciones locales. Este modelo amplio y en el que la coordinación se vuelve un elemento indispensable asegura que las políticas de ciberseguridad sean implementadas de forma coherente a nivel nacional y regional.

Sin embargo, pese al esfuerzo de todos estos organismos, a menudo se presentan dificultades para aquellas corporaciones pequeñas y que disponen de pocos medios. Para ellas es relevante el apoyo que prestan entidades como la Federación Española de Municipios y Provincias (FEMP). Como ejemplo, esta ha elaborado una interesante guía[64], que no es más que un cuaderno de recomendaciones dirigido a las entidades locales de menos de 2 mil habitantes sobre la adecuación a las directrices diseñadas por el Esquema Nacional de Seguridad.

63. Disponible en el siguiente enlace: https://cnpic.interior.gob.es/es/detail-page/articulo/La-Comision-Nacional-para-la-Proteccion-de-Infraestructuras-Criticas-aprueba-el-P.E.A./ (fecha de última consulta: 17/04/2025).

64. Esta guía está disponible en el siguiente enlace: https://ens.ccn.cni.es/es/docman/documentos-publicos/28-femp-tomo-ii/file. Destacan, en todo caso, otras guías, como la Guía estratégica en seguridad para entidades locales, cuyo objetivo, en sus propias palabras, era la creación de una serie de pautas para ayudar a las Administraciones locales a interpretar de forma práctica y homogénea las obligaciones derivadas del Esquema Nacional de Seguridad. Esta última está disponible en el enlace siguiente: https://ens.ccn.cni.es/es/docman/documentos-publicos/27-femp-tomo-i/file (fecha de última consulta: 19/04/2025).

Esta falta de capacidad de las entidades locales más pequeñas es incluso reconocida por alguno de los organismos que analizaremos a continuación, como el propio Centro Criptológico Nacional[65], que afirma que las especiales características que enmarcan la actuación administrativa de las entidades locales más pequeñas, y los limitados recursos con los que cuentan, provocan que la adecuación al Esquema Nacional de Seguridad y su ulterior certificación constituyan obligaciones de difícil cumplimiento de manera individualizada. En este sentido, se ha elaborado el Marco de Certificación ENS para entidades locales, que "persigue la implantación conjunta del ENS en ayuntamientos de la misma provincia, de características tecnológicas y administrativas similares", con el objetivo de "alcanzar la Certificación de Conformidad con el ENS para los sistemas de información de tales ayuntamientos que, en principio, soporten los servicios municipales que se ofrezcan a través de Sede Electrónica"[66].

A este respecto, como señala Almeida Cerreda (2023: 76), en el vigente ordenamiento local existe una importante laguna, por cuanto no se contemplan, de modo específico, las relaciones intermunicipales que pueden ser un importante medio para que los pequeños municipios afronten, de forma conjunta o apoyándose en un ayuntamiento de mayores dimensiones, el desempeño de las funciones y la erogación de los servicios que les encomiende la normativa, a los efectos que aquí nos interesa, en el ámbito de la ciberseguridad.

### 4.1. El Centro Criptológico Nacional (CCN) y su apoyo a las corporaciones locales

El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), es uno de los organismos más relevantes en el entorno de la ciberseguridad en España. Su origen se remonta a comienzos de siglo, y la norma —en este caso reglamentaria— que le sirve de soporte es el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional[67].

65. Sobre la cuestión, se puede consultar: https://ens.ccn.cni.es/es/entidades-locales (fecha de última consulta: 19/04/2025).

66. Todo ello, recogido en la página 1 del precitado documento, disponible en el siguiente enlace: https://ens.ccn.cni.es/es/docman/documentos-publicos/abstracts/29-marco-de-certificacion-ens-para-entidades-locales/file (fecha de última consulta: 26/04/2025).

67. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2004-5051&p=20040319&tn=1 (fecha de última consulta: 26/04/2025).


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

Su misión principal, tal y como reza el artículo 2 del Real Decreto citado, será, en primer lugar, la protección de la seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifrado; y, en segundo término, la seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada. Así pues, el CCN se encarga de establecer directrices de seguridad en materia de protección de redes y sistemas de comunicación del sector público y de la Administración.

Entre las funciones que se la asignan, se encuentra la constitución del organismo de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito (artículo 2.2, letra c). Es decir, será el CCN el que se encargue, según el artículo 19 del Real Decreto 311/2022, de determinar los requisitos funcionales de seguridad y del aseguramiento de la certificación; de otras certificaciones de seguridad adicionales que se requieran normativamente; y, de manera excepcional, del criterio a seguir en los casos en que no existan productos o servicios certificados.

Este cobra también importancia en el ámbito de la administración digital, pues en virtud del artículo 35.2 del Real Decreto que regula el Esquema Nacional de Seguridad, citado en el párrafo anterior, el CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Conviene finalmente traer a colación uno de los elementos que comentamos *ut supra*[68]: la existencia del CCN-CERT, que se constituye como el equipo de respuesta a incidentes que afecten a organismos públicos y sectores estratégicos —a diferencia del INCIBE-CERT, que referenciaremos en el siguiente subepígrafe—. Pues bien, en virtud del artículo 33 del Real Decreto que regula el Esquema Nacional de Seguridad, relativo a la capacidad de respuesta a incidentes de seguridad, el CCN deberá articular la contestación a los incidentes de seguridad en torno a la estructura denominada CCN-CERT, que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración pública, y de la función de coordinación a nivel nacional e internacional del CCN.

68. Concretamente en el apartado 2.1 del presente capítulo.


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

En el papel que el CCN ha asumido de autoridad técnica de referencia en materia de ciberseguridad para el sector público, el CCN-CERT —como unidad operativa-—, por un lado, presta asistencia técnica[69] a ministerios, organismos autónomos, Administraciones autonómicas y locales, universidades públicas y empresas públicas; y, por otro, elabora las denominadas series CCN-STIC[70]. Estas últimas son normas, instrucciones, guías y recomendaciones —de carácter técnico— desarrolladas con el fin de mejorar el grado de ciberseguridad de las organizaciones, por lo que periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT. En el ámbito del apoyo brindado a las corporaciones locales, destacamos la "Guía de Análisis de Riesgos para Entidades Locales", o la "Guía de Implantación del ENS para Entidades Locales", publicadas ambas en el año 2020 con los números 882 y 883, respectivamente. La última de ellas, por cierto, con anexos que concretan el plan de adecuación en función de la dimensión y los recursos de los ayuntamientos, diferenciando entre los de menos de 5 mil habitantes; los que se encuentran entre 5 mil y 20 mil habitantes; los que están entre 20 mil y 75 mil habitantes; y, tras ellos, las diputaciones, cabildos, consejos insulares u órgano competente equivalente, por cuanto también pertenecen a la Administración local en virtud de los artículos 140 y siguientes de la Constitución Española.

A colación de la relevancia que la FEMP tiene en el ámbito de la prestación de apoyos a las entidades locales en materia de ciberseguridad, huelga destacar la colaboración habitual que mantiene con el propio CCN. Esta ha dado lugar a documentos que sirven de apoyo en la labor diaria de los municipios y provincias con la finalidad de, por ejemplo, "precisar la realidad de los riesgos y amenazas que, para el normal desarrollo de los procedimientos administrativos, las funciones involucradas en el desarrollo institucional provincial o municipal y la gestión y administración de las entidades locales, emanan del ciberespacio"[71].

69. En el marco de esta asistencia técnica proporciona herramientas de detección de amenazas, como la plataforma REYES, que permite agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas, como se puede comprobar en el siguiente enlace: https://www.ccn-cert.cni.es/es/soluciones-seguridad/reyes.html (fecha de última consulta: 19/04/2025).

70. El catálogo de dichas normas de carácter técnico está disponible en el siguiente enlace: https://www.ccn-cert.cni.es/es/guias.html (fecha de última consulta: 19/04/2025).

71. Como recoge el Prontuario de ciberseguridad para entidades locales en su página 4, que está disponible en el siguiente enlace: https://ens.ccn.cni.es/es/docman/documentos-publicos/25-ccn-cert-prontuario-ciberseguridad/file (fecha de última consulta: 19/04/2025).


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

### 4.2. El Instituto Nacional de Ciberseguridad (INCIBE) y la ciberseguridad operativa

El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital. Concretamente estamos frente a una sociedad mercantil estatal cuya denominación social es "S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A." y que se rige por sus Estatutos[72], en consonancia con las previsiones del Real Decreto Legislativo 1/2010 de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

Su misión principal es la protección de los ciudadanos, las empresas y las entidades del sector privado frente a los ciberataques. El INCIBE actúa, por tanto, como certificador de ciberseguridad para el sector privado, y gestiona el centro de respuesta ante incidentes de seguridad cibernética denominado INCIBE-CERT.

El INCIBE, y aquí es donde se halla una de sus funciones más relevantes, también fomenta la educación en ciberseguridad mediante programas de formación para empresas[73] y profesionales del sector, así como programas de sensibilización dirigidos a los ciudadanos, y colabora de forma habitual con las universidades, financiando, incluso, programas de investigación y transferencia en la materia.

Como es obvio, su relevancia para las corporaciones locales es infinitamente inferior a la del CCN. Con todo, siguen existiendo puntos de encuentro en donde la colaboración con este organismo se vuelve de interés. Como ejemplo, los convenios de colaboración firmados con diferentes ayuntamientos que se centran en la divulgación y capacitación sobre ciberseguridad para las empresas y para la ciudadanía[74]. En el marco ahora comentado, destacamos el convenio firmado en el año 2024 con el Ayuntamiento de La Pola de Gordón, en Castilla y León, para, a grandes rasgos, favorecer la transformación digital del municipio, en donde uno

72. Pueden ser consultados en el siguiente enlace: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe/normativa-interna (fecha de última consulta: 19/04/2025).

73. Por cierto, en lo que concierne a las empresas que trabajan en el ámbito de la ciberprotección, Euskadi triplica la media española e incluso europea, superando las 79 por millón de habitantes, mientras que en el caso de España y Europa esta cifra se sitúa en 28 y 22,8 empresas por millón de habitantes, respectivamente. Estos datos se pueden observar en las conclusiones del "Libro Blanco de la Ciberseguridad en Euskadi 2024", publicado por la Agencia Vasca de Ciberseguridad, ya citada.

74. Algunos de ellos pueden consultarse en el siguiente enlace: https://www.incibe.es/incibe/tags/convenio%20-%20acuerdo%20colaboraci%C3%B3n (fecha de última consulta: 19/04/2025).

de los puntos clave era la creación de un centro de formación y *coworking* en Santa Lucía de Gordón.

En el ámbito de la ciberseguridad operativa, el Cuerpo Nacional de Policía (CNP) y la Guardia Civil desempeñan roles fundamentales en la investigación y persecución de delitos cibernéticos. Ambas fuerzas cuentan con unidades especializadas en cibercrimen, como la Brigada Central de Investigación Tecnológica (UIT) del CNP y el Grupo de Delitos Telemáticos de la Guardia Civil. Estas unidades tienen la responsabilidad de identificar, investigar y desmantelar redes criminales que operan en el ciberespacio, con especial énfasis en fraudes informáticos, ataques a infraestructuras críticas, y delitos de odio o terrorismo en línea. Sin embargo, de nuevo nos encontramos aquí con una serie de escollos que no renunciamos a enunciar.

De forma breve, gran cantidad de estos delitos son denunciados ante las Policías Locales, cuyos medios para las tareas de averiguación e investigación son ínfimos[75], lo que motiva que deriven sus informes o atestados —en donde se detallan los hechos, el relato del denunciante, otras gestiones realizadas en *pro* de la investigación, aportación de pruebas, extractos bancarios y otra documentación anexa— a las FCSE con capacidad en la materia, nombradamente Guardia Civil y CNP, sin recibir el correspondiente *feedback*, y sin una clara interlocución entre ellos. Así pues, las menores capacidades de la Policía Local de las corporaciones municipales y las deficientes vías de interlocución con otras FCSE, que a menudo dependen de la buena sintonía personal, dificultan la persecución efectiva de los delitos cometidos en el ámbito cibernético.

### 4.3. Otros órganos de relevancia: del Centro Nacional de Protección de Infraestructuras Críticas al Consejo Nacional de Ciberseguridad

Como ya se ha reconocido en diversas ocasiones, la organización española en materia de ciberseguridad no es ordenada ni responde a elementos claros. La gran cantidad de órganos y comités existentes impide centrarse con detalle en cada uno de ellos, motivo por el que nos detendremos,

75. Aunque con el paso del tiempo, y la evolución de las tecnologías, los diferentes integrantes de la Policía Local en España gozan de formación en el ámbito de la ciberseguridad. Normalmente, a partir de los organismos autónomos —en gran medida—, que congregan la capacidad formativa de las FCSE en las diferentes autonomías. A modo de ejemplo, los cursos ofrecidos en la Academia Galega de Seguridade Pública, o la formación ofrecida en el marco del III Encuentro de Policías Locales de Castilla y León, que contó con la colaboración del propio INCIBE.


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

de manera sucinta, únicamente en algunos que, por su alcance material, subjetivo, o por su propio interés sectorial, conviene resaltar.

El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) es otro organismo clave en la defensa de las infraestructuras esenciales para el funcionamiento del Estado. El CNPIC trabaja bajo la supervisión del Ministerio del Interior y tiene como principal objetivo la identificación, protección y resiliencia de las infraestructuras críticas del país, que incluyen sectores como la energía, la sanidad, el transporte, las finanzas y las comunicaciones, como hemos abordado en otro de los epígrafes de este capítulo. Este centro, que nació en el año 2007, se encarga de coordinar la respuesta ante incidentes de ciberseguridad que puedan afectar a estos sectores estratégicos. Gracias al Plan Estratégico Sectorial de la Administración, ya citado, se culminó el Sistema de Protección de Infraestructuras Críticas, lo que facilita la labor del centro a la hora de hacer frente a los entornos multiamenaza existentes.

En segundo término podemos destacar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado[76], que tendrá a su alcance la totalidad de las entidades usuarias del Servicio Unificado de Comunicaciones de la Administración General del Estado, además de otras entidades que cuentan con conexión directa a un nodo de interconexión de la Red de Sistemas de Aplicaciones y Redes para las Administraciones —la conocida Red Sara—, lo que engloba a las propias corporaciones municipales. En palabras del Plan de Digitalización de las Administraciones Públicas 2021-2025, "este centro ayudará a mejorar la seguridad de todas las entidades y además facilitará el cumplimiento del Esquema Nacional de Seguridad al gestionar la seguridad de todas las entidades de manera centralizada", pues en el seno de la medida 9 de dicho plan se encontraba el refuerzo de las capacidades de prevención y reacción ante incidentes de seguridad, así como el incremento de la capacidad de vigilancia y detección de ciberamenazas de un modo centralizado más eficiente, que implique un ahorro significativo de dinero, esfuerzo y tiempo a través del citado centro. A nivel nacional existe, por cierto, una red que los conecta y que actúa como un instrumento para coordinar la colaboración y el intercambio de información entre los centros de operaciones de ciberseguridad del territorio nacional, bien sean públicos o privados. Esta Red Nacional

76. Sobre estos centros, existe un interesante documento elaborado por el Centro Criptológico Nacional, disponible en el siguiente enlace: https://www.ccn.cni.es/ca/docman/documentos-publicos/488-soc-centros-de-operaciones-de-ciberseguridad-infografia/file (fecha de última consulta: 19/04/2025).


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

de Centros de Operaciones de Seguridad tiene, fundamentalmente, el objetivo de integrar y coordinar la cooperación y el intercambio de información entre los mismos, y mejorar las capacidades nacionales de defensa, detección y respuesta a posibles ciberincidentes, y a ella podrán adherirse entidades públicas, proveedoras o privadas[77] que estén bajo la protección de uno de estos centros, bien sea externo o propio.

En tercer lugar, el Consejo Nacional de Ciberseguridad[78] —creado por Acuerdo del Consejo de Seguridad Nacional de 5 de diciembre de 2013[79]— juega un papel crucial en la toma de decisiones a nivel político y estratégico, pues estamos frente a un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. Aunque sus reuniones tienen, como mínimo, carácter bimestral, este puede reunirse cuantas veces sea necesario, a juicio de su presidente y en función de las circunstancias que afecten a la ciberseguridad. Por ejemplo, dicho consejo mantuvo una reunión el 11 de marzo del año 2024 a fin de abordar las diversas iniciativas normativas de ciberseguridad europeas, entre las que se encontraba la transposición de la Directiva NIS 2 al ordenamiento jurídico español, con la que iniciamos este capítulo.

Finalmente, entre otros muchos órganos —ya hemos criticado líneas atrás el excesivo número de centros, comités y consejos, entre otros, con competencias en el ámbito de la ciberseguridad—, podemos destacar dos.

En primera instancia, la Comisión Permanente de Ciberseguridad[80], que —como órgano de asistencia al Consejo Nacional de Ciberseguridad

77. Según se extrae de la propia página web oficial del CCN, citada en el pie de página anterior, en cuanto a las entidades públicas nos hallamos ante organismos de la Administración pública cuyos servicios de seguridad son prestados, generalmente, por proveedores contratados. Sin embargo, cuando nos referimos a entidades proveedoras, nos referimos a empresas del sector privado que prestan servicios actuando como centros de operaciones en otras entidades, ya sean públicas o privadas, protegiendo activos españoles; mientras que con el concepto "empresas del sector privado" nos referimos a aquellas que cuentan con un centro de operaciones propio.

78. Sobre él se contiene diversa información en la página web del Departamento de Seguridad Nacional, disponible en el siguiente enlace: https://www.dsn.gob.es/es/estructuras-de-seguridad-nacional/comites-especializados/consejo-nacional-de-ciberseguridad (fecha de última consulta: 19/04/2025).

79. Aunque fue modificado a finales de la década pasada por la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad, disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2018-799 (fecha de última consulta: 19/04/2025).

80. Existen comisiones permanentes en ámbitos muy diferenciados. Sin ir más lejos, y en estricta conexión con las amenazas híbridas, la Comisión Permanente contra la Desinformación, referenciada en el Informe Anual de Seguridad Nacional del año 2023, disponible


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

sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad, de las autoridades públicas competentes o de los CSIRT— facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad. De este modo, la estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida, tal y como recoge el capítulo V de la Estrategia Nacional de Ciberseguridad del año 2019, por el Consejo de Seguridad Nacional; el Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis; el Consejo Nacional de Ciberseguridad; la Comisión Permanente de Ciberseguridad ahora citada; el Foro Nacional de Ciberseguridad; y las autoridades públicas competentes junto a los CSIRT de referencia nacionales.

En segundo término, destacamos la Oficina de Coordinación de Ciberseguridad, organismo dependiente de la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad, a través del cual se ejecutan las políticas de ciberseguridad del Ministerio del Interior y que, entre sus funciones, incluye la respuesta a las amenazas contra la ciberseguridad, la cibercriminalidad y las campañas de desinformación, así como su actuación en calidad de Observatorio de la Cibercriminalidad del propio Ministerio[81].

Para finalizar, en el ámbito estrictamente castrense nos encontramos con el Mando Conjunto del Ciberespacio, que será el órgano responsable del planeamiento, dirección, coordinación, control y ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial. En dicho mando, por cierto, se encuentra enmarcado el Centro de Respuesta ante Incidentes del Ministerio de Defensa, denominado ESPDEF-CERT.

Pese a su nomenclatura actual, que viene dada por el Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas[82], su origen radica en el Mando Conjunto de Ciberdefensa —creado por la Orden Ministerial 10/2013, de 19 de febrero—, en un

en el siguiente enlace: https://www.dsn.gob.es/sites/default/files/documents/ACCESIBLE%20MAQUETA%20IASN2023.pdf (fecha de última consulta: 19/04/2025).

81. Que tiene como objeto monitorizar y detectar tendencias para hacer frente a nuevos retos y amenazas en dicho ámbito, recopilar, procesar y analizar información sobre ciberseguridad, cibercriminalidad y campañas de desinformación, con la finalidad de elaborar productos de inteligencia, así como planes preventivos y de respuesta, como recoge su página web oficial: https://occ.ses.mir.es/publico/occ (fecha de última consulta: 16/04/2025).

82. De esta forma, según su artículo 9, el Estado Mayor de la Defensa se estructurará en un Cuartel General y en los siguientes órganos: el Mando de Operaciones, el Centro de Inteli-

contexto en el que, según la Estrategia de Seguridad Nacional vigente por aquel entonces, los ciberataques comenzaban a ser "una amenaza actual, real y en crecimiento para los intereses nacionales". Por todo ello, según el artículo 15 del derogado Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas, se designaba al Mando Conjunto como el responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa, u otras que pudiera tener encomendadas, así como el encargado de contribuir a una respuesta adecuada en el ciberespacio ante amenazas o agresiones que pudieran afectar a la Defensa Nacional. En conexión con lo anterior, y según el análisis literal de la orden citada, este mando tenía encomendada la cooperación con los centros nacionales de respuesta a incidentes de seguridad de la información.

## 5. Conclusiones

La normativa española en el ámbito de la ciberseguridad encuentra su acomodo en las directrices previamente marcadas por la Unión Europea, lo que resulta, sin duda, positivo. Partiendo de que el concepto de ciberseguridad trasciende lo técnico e integra también dimensiones políticas, jurídicas, organizativas y sociales, de que es un fenómeno global y dinámico, y de que esta es clave para garantizar el funcionamiento del Estado de derecho, también en la escala local, por su creciente exposición a amenazas, la homogeneidad en el ecosistema europeo promueve una respuesta estructurada.

Sin embargo, ello depende en buena medida de la transposición que el legislador nacional realice de la Directiva NIS 2, que esperemos se produzca a la mayor brevedad, tal y como adelantaba a comienzos de año el Ejecutivo español, y que traerá consigo novedades como la creación de un Centro Nacional de Ciberseguridad que ejerza de autoridad central y que, en función de su diseño, podrá facilitar la coherencia del sistema español —entendido *lato sensu*— o fomentar la amalgama organizacional imperante en la materia.

Sea como fuere, en la actualidad el Real Decreto-ley 12/2018 es el que constituye el eje normativo principal que, de la mano del resto de normas, documentos y planes existentes en la materia —algunos de ellos de acceso

gencia de las Fuerzas Armadas, el Mando Conjunto del Ciberespacio, y el Centro Superior de Estudios de la Defensa Nacional.


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

restringido—, sirve de paraguas legislativo a las Administraciones locales, que son especialmente vulnerables por su limitada capacidad técnica y presupuestaria, lo que las convierte en objetivo frecuente de ciberataques. No debe olvidarse que, fruto de la entrada en vigor de la futura Ley de Coordinación y Gobernanza de la Seguridad, este real decreto-ley quedará derogado —al igual que el reglamento que le sirve de desarrollo— en virtud de la disposición derogatoria única del anteproyecto de la propia norma.

Por ello, son relevantes los esfuerzos que se han hecho en pro de la seguridad de las corporaciones municipales, y en particular, de los pequeños municipios. Pese a que, como decimos, existen elementos positivos, muchas de las normas que regulan la materia exigen meras formalidades que, *de facto*, no tienen gran valor añadido frente a ciberamenazas reales. A modo de ejemplo, las políticas de seguridad de los ayuntamientos o diputaciones.

En lo que a la propia organización de la ciberseguridad en España se refiere, también son múltiples los centros, organismos y órganos que comparten competencias y funciones en la actualidad. El panorama estatal en este contexto es difícil de desgranar; por eso resulta de vital importancia la coordinación y colaboración entre los mismos —y también con empresas privadas— a efectos de evitar o reducir al mínimo el riesgo de solapamientos en el ámbito competencial, y de buscar la mayor resiliencia en la lucha contra las ciberamenazas.

En definitiva, aunque España cuenta con mecanismos legislativos y operativos diversos, analizados los más relevantes en este capítulo, es imprescindible que los poderes públicos realicen un análisis que intente poner orden en un ecosistema que, aunque defendemos que sea descentralizado, debe ser coherente y único, y tener en cuenta las necesidades de aquellas entidades de menor tamaño que, *per se*, no pueden hacer frente a las amenazas que se plantean en el ciberespacio con las mismas facilidades que las grandes corporaciones.

## 6. Bibliografía

Adeva, A. y Vera, J. M. (2024). Organización de la Ciberseguridad: quién lleva la batuta. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, 33 (159), 98-107.

Almeida Cerreda, M. (2023). Un posible régimen especial para los pequeños municipios: justificación, naturaleza, contenido y articulación. *Re-*



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

*vista de Estudios de la Administración Local y Autonómica: Nueva Época*, 19, 59-81.

Almeida Cerreda, M. (2024). Las relaciones entre Administraciones públicas. En F. Velasco Caballero y M. M. Darnaculleta Gardella (dirs.). *Manual de Derecho administrativo* (pp. 321-346). Marcial Pons.

Almeida Cerreda, M. (2025). *La regulación de la ciberseguridad en España: reglas, actores e instrumentos*. Lección impartida en la Universidad de Palermo. [Manuscrito inédito], 1-21.

Álvarez Robles, T. (2024). La ciberseguridad: la seguridad integral y descentralizada del estado digital. En F. Caamaño y D. Jove Villares (dirs.). *Tecnologías abusivas y derecho* (pp. 255-293). Tirant lo Blanch.

Blesa López, A. (2018). *España y sus Estrategias de Seguridad (2000-2017): un análisis comparativo*. Instituto Español de Estudios Estratégicos. Disponible en https://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO75-2018_Espana_EstrategiasSeguridad_AnaBlesa.pdf.

Canals Ametller, D. (dir.). (2021). *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales*. El Consultor de los Ayuntamientos.

Fernández Rodríguez, J. J. (2018). Ciberseguridad: ¿desafío insuperable? En búsqueda de escenarios de respuesta adecuados. En C. García Novoa y D. Santiago Iglesias (dirs.). *4ª Revolución Industrial: impacto de la automatización y la Inteligencia artificial en la sociedad y en la economía digital* (pp. 51-80). Aranzadi.

Fernández Rodríguez, J. J. (2023). Reflexiones (provisionales) sobre los derechos de los robots. En M. A. Rocha Espíndola, D. Sansó-Rubert Pascual y N. Rodríguez Dos Santos (coords.). *Inteligencia artificial y derecho. Reflexiones jurídicas para el debate sobre su desarrollo y aplicación* (pp. 227-242). Dykinson.

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

Jareño Butrón, M. y Arratibel Arrondo, J. A. (2024). Recomendaciones de la Agencia Europea de Ciberseguridad ante incidentes de seguridad en el sector sanitario. *Auditoría pública: revista de los Órganos Autónomos de Control Externo*, 83, 115-137. Disponible en https://asocex.es/wp-content/uploads/2024/05/10-RECOMENDACIONES_.pdf.

Rebollo Puig, M. (2019). La trama de la Ley de Seguridad Ciudadana. En M. Izquierdo Carrasco y L. Alarcón Sotomayor (dirs.). *Estudios sobre la Ley Orgánica de Seguridad Ciudadana* (pp. 31-170). Aranzadi.

Rodríguez González, V. (2024). La seguridad nacional frente a nuevas modalidades delictivas. *Blog de la Universidad Isabel I*. Disponible en https://www.ui1.es/blog-ui1/la-seguridad-nacional-frente-nuevas-modalidades-delictivas.



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